UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	**No. 08 CR 192**
v.	)	
	)	**Judge Ruben Castillo**
HANJUAN JIN,	)	
	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

On December 9, 2008, a Grand Jury returned a superseding indictment charging Hanjuan Jin ("Defendant" or "Jin") with three counts of theft of trade secrets and three counts of economic espionage in violation of the Economic Espionage Act, 18 U.S.C. § 1831 *et seq.* ("EEA"). (R. 37, Superseding Indictment.) On November 7, 2011, Jin voluntarily waived her right to a jury trial and proceeded to a bench trial, which was held from November 7, 2011, to November 15, 2011. The Court, having reviewed all of the evidence, its trial notes, the testimony of the witnesses to determine the credibility of each witness, and the parties' post-trial submissions, hereby concludes that Jin criminally betrayed Motorola by stealing its trade secrets. The Court also concludes that there was not enough evidence to find that Jin criminally betrayed the United States by committing economic espionage for the Peoples' Republic of China ("PRC"). The Court enters the following findings of fact and conclusions of law pursuant to Federal Rule of Criminal Procedure 23(c).

BACKGROUND

A criminal complaint was filed against Jin on March 3, 2008. (R. 1, Compl.) On April 1, 2008, Jin was indicted by the Grand Jury. (R. 11, Indictment.) On December 9, 2008, the Grand Jury returned a superseding indictment (the "indictment"). (R. 37, Superseding Indictment.)

The indictment alleged that Jin began working as a software engineer for Motorola, a telecommunications company based in Chicago, in 1998.[1] (*Id.* at 1.) In February 2006, Jin took a one-year medical leave of absence from Motorola. (*Id.* at 2.) According to the indictment, during this time, Jin negotiated and ultimately accepted employment with Sun Kaisens, a telecommunications company in China that develops telecommunications technology and products for the Chinese military.[2] (*Id.* at 1-2.) The indictment further alleged that after accepting employment with Sun Kaisens, Jin briefly returned to work at Motorola at the end of February 2007, downloaded numerous Motorola proprietary technical documents, and was in possession of those documents as she attempted to board a flight to China on February 28, 2007. (*Id.* at 2-3.)

According to the indictment, three of the documents in Jin's possession, Moto 1, Moto 2, and Moto 3, were trade secrets. Counts One through Three—one count for each document—charged Jin with possession of trade secrets with intent to convert them to the economic benefit of someone other than the owner, intending or knowing that the offense would injure the owner, in violation of 18 U.S.C. § 1832(a)(3) ("Section 1832(a)(3)"). (*Id.* at 1-6.) Counts Four through Six—again, one count for each document—charged Jin with possession of

[1] The indictment refers to Motorola as "Company A." For ease of reference, the Court will use Motorola instead of Company A throughout this opinion.

[2] The indictment refers to Sun Kaisens as "Company B." For ease of reference, the Court will use Sun Kaisens in place of Company B in this opinion.

trade secrets, knowing the trade secrets were obtained and converted without authorization, intending or knowing that the offense would benefit a foreign Government, in violation of 18 U.S.C. § 1831(a)(3) ("Section 1831(a)(3)"). (*Id.* at 7-9.) In sum, the indictment alleged that Jin stole trade secrets pertaining to telecommunications technology from Motorola, and intended to convert those trade secrets to the benefit of herself, Sun Kaisens, and the PRC.

FINDINGS OF FACT

The Court concludes that the Government established by both direct and circumstantial evidence, as well as reasonable inferences therefrom, the following facts beyond a reasonable doubt:

Jin's employment with Motorola

1. Jin attended the University of Science and Technology of China, and received her bachelor of science in physics. She received her master's degree in physics from the University of Notre Dame. (Govt. Ex. MBR 3; Tr. 349.)

2. On June 16, 1998, Jin began working at Motorola as a software engineer in the iDEN-Systems Integration & Test department. (Govt. Ex. MBR 3.) iDEN is a proprietary standard for cellular telecommunications technology developed by Motorola.

3. In January 2000, Jin received a rating of "Met All Expectations" on her performance review. Her 2001 rating was "Exceed Expectations" and "Solidly Effective." In 2002, she received a rating of "Meets all, exceeds some" and "Solidly Effective." In 2003, her rating was "Exceed Expectations" and "Most Effective." She was rated as "Excellent" in 2004, and "Effective" in 2005. (Govt. Ex. MBR 3.)

4. Over the course of her employment with Motorola, Jin received eight merit

increases in her salary, two hierarchy promotions, and a special adjustment. In 2005, prior to her moving to a part-time schedule, her annual salary was $87,136. (Govt. Ex. MBR 3.)

Jin's work for Lemko

5. While employed by Motorola and in contravention of Motorola's policies, Jin worked for Lemko, another telecommunications company. In August 2004, Jin did consulting work for Lemko. (Tr. 657.) The following year, in March 2005, Jin began working as an employee of Lemko. (Tr. 653.) This position with Lemko introduced Jin to the work of Sun Kaisens in China.

6. From April 26, 2005, through May 2, 2005, Jin traveled to Beijing on business for Lemko with Beth Zhang and Shaowei Pan, the Chief Technology Officer of Lemko. (Tr. 595, 641.) Jin, Zhang, and Pan worked with Sun Kaisens to test CDMA technology on this trip. They did not work on any technology for the Chinese military. (Tr. 642-45.)

7. In May 2005, Jin began working part-time for Motorola. On June 15, 2005, Jin took an unpaid medical leave of absence from Motorola. (Govt. Ex. MBR 3.) Motorola prohibits employees on medical leave from performing work for Motorola. (Tr. 503.) Jin returned from leave on September 1, 2005. (Govt. Ex. MBR 3.)

8. On November 13, 2005, Jin took a second trip to China for Lemko with Zhang and Pan. (Tr. 595, 642; Govt. Ex. UAL 1.) On this trip, they continued to work on the same CDMA technology with Sun Kaisens. (Tr. 642.) Jin returned from China on November 28, 2005. (Govt. Ex. UAL 1; Tr. 595.)

9. In February 2006, Jin was diagnosed with meningitis. (Tr. 663.) On February 15, 2006, Jin took another unpaid medical leave of absence from Motorola. (Govt. Ex. MBR 3.) In

March 2006, Jin was hospitalized for 21 days for the very serious condition of meningitis caused by tuberculosis. Her recovery while in the hospital and in the months following was rocky and complicated. She was placed in isolation and needed a tube inserted in her skull to relieve the pressure on her brain.

10. Jin was hospitalized for a second time that summer, and it was discovered that she had suffered a small stroke. In October 2006, Jin's doctor recommended that Jin not work full-time, though she believed Jin could work for brief periods. She did not place any restrictions on Jin's travel. (Tr. 664-66.)

11. Over the course of the next year, Jin downloaded numerous Chinese-language documents related to telecommunications technology, the Chinese Military, and Sun Kaisens onto her laptop, an Ion hard drive, and a thumb drive. On June 1, 2006, she saved the document "A Comparison of China's Digital Trunked Systems" onto her Ion hard drive. (Govt. Exs. MH 1, ION 11.)

Jin's potential employment with Sun Kaisens

12. During the summer of 2006, Jin began corresponding with Sun Kaisens management about possible employment at Sun Kaisens. The emails make it clear that Jin was eager to obtain a job with Sun Kaisens, and was making plans to move back to China. Her health problems, however, caused her to repeatedly push back her move date. In one email to Chief Qi, a Sun Kaisens manager, Jin wrote about the health problems she was experiencing and her hope of returning to China by the end of August. She apologized for the trouble she had caused for Chief Qi's "work arrangement," and requested "documents related to the project" to prepare herself at home. (Govt. Ex. LAP 2 TR.)

13. Jin's health problems continued to delay her move to China. On September 9, 2006, Jin sent another email to Chief Qi. In the email, she expressed regret for having to postpone her return date to China once again, and discussed her recovery. She wrote, "[b]y the time I join your team, I will be in high spirits as well as in good physical condition." She also expressed interest in purchasing a home in Beijing and prior to that, renting a place near Sun Kaisens. She hoped to arrive in Beijing by October 1st. (Govt. Ex. LAP 2 TR.)

14. In an email dated November 6, 2006, Jin expressed relief that she finally had a solid return date to China after several postponements. She stated that she planned to resign from Lemko the following week and return to China on October 16th. She wrote that she would visit her mother and try to arrive in Beijing by the end of the month. She also requested a formal letter of appointment from Chief Qi. (Govt. Ex. LAP 2 TR.)

15. On November 9, 2006, Jin saved the Sun Kaisens document "Next Generation Soft-Switching Technology Program Version 1.0," dated August 2006, onto her thumb drive. (Govt. Exs. MH 1, THD 6.)

16. Jin traveled to China on November 16, 2006. (Govt. Ex. UAL 1; Tr. 596.) While the full details of what occurred on this trip were not established at trial, it is clear that Jin continued to pursue a position with Sun Kaisens and even completed work for the company. Jin met with Gengshan Liu, a Sun Kaisens manager with whom she had met on her previous trips to China in 2005. At this meeting, Liu provided Jin with numerous Chinese documents that were found in Jin's possession on February 28, 2007. He asked Jin to review the documents and ascertain how much assistance she could provide on the projects. Jin viewed this as a probationary period, and told Liu that she would provide him with the work when she finished.

Jin also visited the Sun Kaisens office during this trip. (Tr. 146-49.)

17. Around this time, Jin obtained a Sun Kaisens email account. (Govt. Ex. LAP 5 TR.) On December 4, 2006, Liu sent Jin an email at her Sun Kaisens email address. (Govt. Ex. LAP 3 TR.) In the email, Liu asked Jin to familiarize herself with an attachment to the email, a document entitled "Softswitching Motorized System Technical Requirement (draft).doc," which Liu said was going to be discussed with "Institute 61 and other units." (Govt. Ex. LAP 3 TR.) The 61st Research Institute is under the oversight of the Chinese military and develops equipment for the People's Liberation Army ("PLA"). (Tr. 564.)

18. Over the course of the next few days, Jin received emails at her Sun Kaisens account and saved several Chinese military and Sun Kaisens documents, later found in her possession, onto her electronic data storage devices. On December 4, 2006, Zhang emailed Jin at her Sun Kaisens email address. (Govt. Ex. LAP 1 TR.) On December 14, 2006, Jin saved a document entitled "An Introduction to SM2000 System, Portable Military Mobile Cellular Communication System, Economical Mobility Mobile System," onto her Ion hard drive. (Govt. Ex. MH 1.) On December 15, 2006, Jin received an email from Zhang with a project update. (Govt. Ex. LAP 6 TR.) That same day, Jin saved documents entitled "Comprehensive Military Communications System 2nd General Meeting Summary" and "Integrated Mobile Communication System, Mobile Switch Development Technical Proposal" (Govt. Exs. ION 3, 4), onto her Ion hard drive, and documents entitled "Combat Use Requirements and Major Tactical Technology Specifications of Military Comprehensive Mobile Communication Systems," "Major Tactical Technology Specifications of Vehicular Mobile Switches of Military Comprehensive Mobile Communication System," and "Major Tactical Technology

Specifications of Portable Mobile Switches of Military Comprehensive Mobile Communication" (Govt. Exs. THD 4, 5, 7) onto her thumb drive. (Govt. Ex. MH 1.)

19. On January 28, 2007, Jin emailed Shaowei Pan and told him that she had been spending time in Shanghai and Beijing. She said that her health had improved, but that her husband did not feel comfortable with her staying in the United States by herself, and that she was thinking about finding a job in Beijing. She said that she would like to work with Chief Qi at Sun Kaisens, and asked that Pan put in a good word for her with Chief Qi. (Def.'s Ex. 1.)

20. On February 8, 2007, Jin saved a Sun Kaisens document listing Jin as a chief director for a Sun Kaisens project (Govt. Ex. ION 6) onto her Ion hard drive. (Govt. Ex. MH 1.) On February 14, 2007, she saved additional Chinese military and Sun Kaisens documents (Govt. Exs. ION 2, 5, 7, and 9) onto her Ion hard drive. (Govt. Ex. MH 1.)

Jin's temporary return to Motorola

21. On February 15, 2007, Jin returned from China. (Govt. Ex. UAL 1; Tr. 596.) The evidence before the Court overwhelmingly showed, however, that she intended for her return to the United States to be short-lived.

22. Over the next two weeks, Jin made preparations to return to China. On February 18 and 19, 2007, Jin accessed 28 files on Compass, a Motorola file sharing program, even though she was still on sick leave. (Govt. Ex. TC Summ 4; Tr. 450.)

23. On February 21, 2007, Jige Chen, Jin's husband, withdrew $10,000 from their Chase bank account. (Govt. Ex. CHA 4.)

24. On February 22, 2007, Jin reserved two one-way tickets to China, one ticket for a flight departing February 26, 2007, and one ticket for a flight departing February 28, 2006.

(Govt. Ex. UAL 10; Tr. 597-98.)

25. The next day, Friday, February 23, 2007, Jin returned to Motorola. She sought to end her medical leave and return to work. (Tr. 503.) The direct and circumstantial evidence overwhelmingly establishes, though, that Jin did not in fact intend to work for Motorola. Rather, her return was a mere pretext to obtain thousands of Motorola proprietary documents, including the charged documents.

26. When Jin arrived at Motorola that morning, she was stopped by a security guard, who called Linda Ebel, a nurse at Motorola. Ebel went to security, signed Jin in, and brought Jin to her office. (Tr. 503-04.) Jin gave Ebel her return-to-work slip, which was signed by her doctor and dated February 23, 2007. (Tr. 504; Govt. Ex. MBR 23.) Ebel was unable to initiate Jin's return to work, however, because she had already turned Jin's termination status over to Human Resources when Jin's leave had expired the previous week. At Motorola, an employee is normally terminated after twelve months of medical leave. (Tr. 503-06.)

27. Ebel contacted Human Resources, and was told that Jin could return to work. Ebel next contacted Jin's manager, Bob Bach, to see if he was ready to accept Jin that day, but she was unable to reach him. Jin said she would find Bach and start to work, but Ebel said that she could not permit that because Jin first needed Bach's approval to return to work. Ebel continued to attempt to reach Bach, but to no avail. Jin once again asked if she could go find Bach and start working, but Ebel told her that was not possible. She told Jin that she had to take her back down to security, and security could continue to try and contact Bach. Jin complied and Ebel left her with the security guard at around 11:15 a.m. (Tr. 507-08.)

28. After leaving Jin with security, Ebel emailed the Visitor Center Security to advise

them that Jin's security badge could be reactivated based on the decision made by Human Resources. She also emailed Bach to let him know that Jin had left the office. (Tr. 508.)

29. That afternoon, not knowing that her security badge had been reactivated and therefore believing she could not obtain the Motorola documents over the weekend, Jin canceled the ticket reservation for the flight to China leaving on Monday, February 26, 2007, and purchased the ticket for the flight leaving Wednesday, February 28, 2007. (Govt. Ex. UAL 10; Tr. 600.)

February 26, 2007

30. On Monday, February 26, 2007, Jin officially returned to Motorola from her leave of absence. (Govt. Ex. MBR 3.) She met with Bach around 9:00 a.m., and they discussed what had been happening in the iDEN division while she was on leave. Bach did not give her any specific assignments, but asked her to start familiarizing herself with some documentation related to Melody, a project that the iDEN division was working on at the time. He also told her to get her email and accounts up-to-date. Bach told her that he would follow-up with her in a day or two, once he knew what she would be working on. (Tr. 519-20.)

31. Following that meeting, Jin began accessing and downloading thousands of documents, few of which, if any, were related to the Melody project. That morning, she accessed 166 files on Compass, including Moto 3. After leaving and returning to Motorola that afternoon, Jin accessed an additional 64 files, including Moto 1 and Moto 2. (Govt. Ex. TC Summ 4; Tr. 450-51, 457-58.) She then saved 2,909 files onto her Ion hard drive. (Govt. Ex. JD Summ 5.)

32. That evening, Jin returned to Motorola around 8:40 p.m. (Govt. Ex. MBR 1.) She accessed two files on Compass (Govt. Ex. TC Summ 4; Tr. 451), and saved 2,219 files onto

her Ion hard drive, including Moto 1, Moto 2, and Moto 3. (Govt. Exs. JD Summ 5, 7.) At 12:17 a.m., Jin left the building with two large shopping bags. (Govt. Exs. MBR 1, 14; Tr. 463.) She returned immediately, and then left again with an armful of documents. (Govt. Ex. MBR 14.)

February 27, 2007

33. Jin returned to Motorola at around 11:00 a.m. the morning of February 27, 2007. (Govt. Ex. MBR 1; Tr. 463.) At 11:39 a.m., she downloaded 24 files onto her Ion hard drive. (Govt. Ex. JD Summ 5.)

34. At 12:13 p.m., Jin emailed Bach. In the email, which has a subject of "Disappointment decision," Jin wrote:

> Hey, Bob,
>
> It was nice talking with you yesterday. But I'm afraid that I have to disappoint you. Out of working for so long time, I feel that I cannot get used to the pace of working life anymore. I feel exhausted last night after just one workday. Being such physical condition, I am afraid I am not capable of fulfilling any task that you will assign me. Instead of drag the whole group's performance down and disappoint you, I think it is better for me to volunteer the laying off now. If it is not workable, please let me know if there is other alternative. I am still on heavy medication, I need some more time for full recovery. Please let me know your decision ASAP.
>
> Thanks, Hanjuan

(Govt. Ex. BB 3.) Although Motorola had recently undergone a round of reorganization lay-offs, Bach was surprised to receive this email because they had discussed Jin returning to work full time just the previous day. After receiving this email, Bach attempted to contact Jin without success. (Tr. 523-24, 529.)

35. A few hours after sending this email, at 3:06 p.m., Jin withdrew $20,000 from her Chase bank account. (Govt. Ex. CHA 5.)

36. That evening, at 10:10 p.m., Jin returned to the Motorola campus. (Govt. Ex. MBR 1; Tr. 463.) She accessed 119 documents on Compass between 10:49 p.m. and 12:37 a.m. (Govt. Ex. TC Summ 4; Tr. 451.) She saved 1,868 documents onto her Ion hard drive, including Moto 1, 2, and 3 for the second time. (Govt. Exs. JD Summ 5, 7.) She left Motorola at 12:46 a.m. carrying a laptop bag. (Govt. Ex. MBR 14.)

February 28, 2007

37. The following morning, between 5:38 a.m. and 9:51 a.m., Jin saved 124 documents onto her personal laptop. She also saved 2,472 documents onto her hard drive, including three additional copies of Moto 1, 2, and 3. (Govt. Ex. JD Summ 5, 7.) In total, Moto 1, Moto 2, and Moto 3 appeared in five locations on the Ion hard drive. (Tr. 197; Govt. Ex. JD Summ 7.)

38. The documents Jin accessed on the Motorola network between February 26th and the early morning of the 28th fell under three main categories: (1) iDEN; (2) Tetra/Dimetra; and (3) Human Resources job descriptions and grade levels. (Tr. 444; Govt. Ex. TC Summ 2.) Tetra is a public safety standard used for police radios and public safety equipment, and Dimetra is a Motorola product that implements the Tetra standard. Jin accessed approximately 60 documents in this category during this time period. (Tr. 445-46.) Jin also accessed documents related to Motorola's tiered structures of engineering and Motorola's salary structure. (Tr. 446; Govt. Ex. TC Summ 2.) Most of the documents Jin accessed were related to iDEN. (Tr. 447.)

The Stop at O'Hare

39. That afternoon, at around 12:30 p.m., Jin was stopped by U.S. Customs and Border Protection ("CBP") officials at Chicago O'Hare International Airport ("O'Hare") as she attempted to board a flight to Beijing. Officer Nicolas Zamora, who was conducting random examinations of passengers and luggage departing the United States, stopped Jin for a search on the jet bridge as she was boarding the flight. He asked to see Jin's travel documents, asked her a few questions regarding her trip, and informed her of the currency reporting requirements, which require passengers traveling with more than $10,000 to declare the currency with CBP. Officer Zamora asked Jin how much money she was traveling with, and she initially stated she was traveling with $10,000. (Tr. 39-42.)

40. After a few more questions, Officer Zamora gave Jin a form that explains the currency reporting requirements. Jin requested the form in Chinese. After she read it, Officer Zamora asked Jin if she understood the form, she said yes, and Officer Zamora again asked Jin how much money she had with her. Jin then said that she had $11,000. She proceeded to change the amount that she declared on the form from $10,000 to $11,000. She also signed the form, which stated that "Under penalties of perjury, I declare that I have examined this report, and to the best of my knowledge and belief, it is true and correct." (Tr. 43-45, 48; Govt. Ex. HJ 9.)

41. Officer Zamora next asked Jin to present her currency for verification, and she complied. Jin presented Officer Zamora with two bank envelopes from her laptop bag, and each contained $5,000. She also presented him with an additional $1,252 from

her purse. Officer Zamora asked her if this was all the money she had, and Jin said yes. (Tr. 48-49.)

42. Officer Zamora then told Jin that he needed to examine her bags. He found four additional bank envelopes, each containing $5,000, in her laptop bag. Jin said that her husband must have placed the additional money in her bag without her knowledge. In total, Jin was carrying $31,252. (Tr. 49-50.)

43. Officer Zamora told Jin that because she had not properly declared her money with CBP, she would miss her flight while they processed paperwork. He and other CBP officials next searched Jin's carry-on bags, and found Motorola documents marked as "confidential and proprietary information," a laptop, a hard drive and thumb drive storage devices, and other documents in Chinese. (Tr. 50-53; Stipulation 2; Govt. Exs. Air 2, 4-6, 10-15, 17-25, 27.) They also found a bank receipt for a $10,000 withdrawal on February 21, 2007, identification, and other documents. Officer Zamora asked Jin why she had the Motorola documents, and Jin said she had them for work purposes. (Tr. 63-68.)

44. The CBP officers next escorted Jin to their office. They contacted their task force officer, notified the Federal Bureau of Investigations ("FBI"), and informed Jin of her Miranda rights. Jin agreed to be interviewed. The interview was conducted by FBI Agents Robert Klimas and Joe Devuono and lasted for approximately four to five hours. Agents Klimas and Devuono asked Jin about her education, family, and work background. (Tr. 69-70, 98, 100-03.)

45. During this interview, Jin stated that she was a full-time employee at

Motorola, that she had been employed by Motorola since 1998, and that she worked on the iDEN system. Jin also stated that she was planning to travel to China for an undetermined amount of time because of her mother's illness, and that her trip to China was not related to her work at Motorola. (Tr. 103-04.)

46. Jin said that she was carrying the Motorola documents because she wanted to refresh her knowledge of the information contained in the documents as she had been on sick leave for an extended period of time. (Tr. 103-04.) Jin also said that she was not going to give the documents to anyone else, and that she had not thought about the consequences of leaving the United States with the documents. (Tr. 123.) She said that she understood that the Motorola documents marked "confidential and proprietary" belonged to Motorola and that she was prohibited from giving the documents to non-Motorola entities, organizations, or employees. (Tr. 107.)

47. Jin told Agents Klimas and Devuono that she had returned from sick leave in February 2007. She said that she returned from sick leave on Monday, February 26, 2007, and worked full days from 9 a.m. to 6 p.m. on the 26th and 27th. (Tr. 104,107-08.)

48. Jin told the agents that her supervisor was Bob Bach and that she had told him that she was going to China. Agent Klimas then called Bach, and Bach said he did not know that Jin was going to China or taking any kind of trip. When the interview resumed and Agent Klimas told Jin that Bach was unaware of her trip to China, she said that she had told him she was going to be off for a while. (Tr. 108-09.)

49. Jin said that she was not aware of the extra $20,000 found in her luggage, that her husband must have put it there, and that she and her husband had a savings and

checking account at Chase Bank, a savings and checking account at the Motorola Federal Credit Union, and a bank account at the China Merchants Bank. (Tr. 105.)

50. Jin told the agents that she used two email accounts, a Motorola account and chenjige@haimo.com.cn. (Tr. 105.) She did not mention her Sun Kaisens email account.

51. During the interview, Agent Klimas asked Jin about a Motorola handbook regarding proprietary information found in her possession. Jin said that she had never read it, but when asked about the handwriting on the document, Jin acknowledged that it was her handwriting. (Tr. 109-10; Govt. Ex. Air 17.)

52. Jin also told the agents that the laptop she had with her was her own personal computer, not a Motorola-owned personal computer. When Agent Klimas asked her if there were any Motorola documents similar to the ones she possessed in hard copies on her laptop's hard drive, she said there were none. The agents then asked if they could look at the laptop's hard drive, and Jin consented. Agent Klimas proceeded to conduct a search on the laptop for "Motorola," and hundreds of documents came up. They went through the same process on the other storage devices in Jin's possession, and additional Motorola documents marked "confidential and proprietary" were found. At this point, Jin said that she was a part-time worker at Motorola working 20 hours a week and earning an annual salary of $45,000. (Tr. 110-12.)

53. Agent Klimas asked Jin where she obtained the Thales Catalog, a catalog of military technology products, and she said she received it from a friend. Agent Klimas then asked the friend's name, and after a silence of several minutes, Jin said that she was

reluctant to give the name of the friend. After a few minutes, Jin said that she received the catalog from Zheng Shan Liu (spelling provided by Jin) to review and read. Jin said that Zheng Shan Liu was an engineer with an expertise in software development who owned or worked for a company in China. She said that she had met Zheng Shan Liu several years earlier and that she had met him approximately three times. She said that she did not know the name of the company where Zheng Shan Liu was employed, that he did not have any connections with the Chinese government, and that he was in the telecommunications business and purchased cell phones. Jin said that when she had met with Zheng Shan Liu in the past, he asked her about her work at Motorola. (Tr. 113-15.)

54. The agents obtained a translation of the first page of one of the Chinese-language documents, which indicated that the document was classified and related to Chinese military telecommunications systems. Jin said that she did not have any connections with the Chinese government, and that she downloaded the documents from the Internet. When Agent Klimas pressed her again about the origin of the documents, Jin changed her story and said she obtained the documents from Zheng Shan Liu. (Tr. 116-17.)

55. At the end of the interview, Jin was permitted to go home. CBP officials arranged for her to take the same flight the next day.

March 1, 2007

56. The next day, March 1, 2007, Jin was stopped again as she attempted to board a flight to China on the ticket provided by CBP. She was brought to the FBI office at O'Hare, and interviewed for four to five hours by Agent Michael Diekmann. Jin

agreed to the interview. Although there was a translator present, she chose to have the interview in English. When asked about the Motorola documents marked "confidential and proprietary," Jin said that she had them in her possession to refresh her memory and study them while she was in China. She said she had been on sick leave for the previous year, and wanted the documents to help her get her next job. (Tr. 129-134.)

57. Regarding her medical leave, Jin told Agent Diekmann that she had been on sick leave until February 26, 2007. She said that she had told her supervisor that she was ready to return to work and resume her duties, worked a full day on the 26th, and had returned to Motorola that evening to retrieve some personal items. Jin told Agent Diekmann that she had informed her supervisor on the 27th that she was not able to work due to her medical situation, and that she was taking a voluntary layoff. (Tr. 134-35.)

58. When questioned about the classified Chinese documents, Jin told Agent Diekmann that an individual named Fengshan Li (spelling provided by Jin) had given them to her when she was in China in November 2006. She said that Li had given her the documents so that she could determine what type of assistance she could provide on projects related to the documents, which pertained to telecommunications. Jin said that she had first met Li in April 2005 in Beijing, and during that meeting they had discussed technology-related materials. (Tr. 136-37, 141.)

59. Agent Diekmann also asked Jin about the Thales catalog. Jin said that the catalog had been in Li's possession, and that she thought it was interesting and asked to borrow it. (Tr. 138.)

60. At this point in the interview, Agent Diekmann advised Jin of her Miranda

rights, and she agreed to continue with the interview. (Tr. 139.)

61. Agent Diekmann next asked Jin to translate the title of one of the documents. She provided a translation, "Mobile Telecommunications Configuration Management System." The translator told Agent Diekmann that she had not translated the last few characters of the title, and Agent Diekmann asked her to translate the title again. Jin translated the title and added the last two words, "Requirements List." She told Agent Diekmann that the document was created by Sun Kaisens, a company located in Beijing in the business of computers, telecommunication, and information technology. She said that an engineer gave her the document in December 2006. (Tr. 139-40; Govt. Ex. Air 22.)

62. Agent Diekmann also asked Jin about her name being listed on the document, and she acknowledged that her name was listed. The translator said her title on the document was "Project Chief Director," but Jin disagreed with that translation and said the actual title was "Director of Guidance." Jin said that she had previously assisted Sun Kaisens on similar projects. (Tr. 140-41.)

63. At the end of the interview, Jin provided a signed and dated handwritten statement. The statement reads as follows:

> I have some Motorola documentation, they are related with the work that I have done these years in Motorola. I have been sick and took medical leave for a year and more. I felt so lack of sense of job that I had done. I plan to take vacation to China and visit my mom who is not well. I took the papers that I had in my cabinet with me for the trip. The only purpose that I have the papers is that I can refresh the work that I have done these years so that I can prepare myself for further career going. I swear that I have no intention to cause any damage to Motorola.
>
> In my baggage I also had some Chinese paper with me. They are papers that were given to me for reviewing by my friend. He wanted to help with the project

using my expertise. I have not done anything yet. My friend name is Fengshan Li.

Officers also asked me a lot of questions about import/export. I am very lacking of knowledge of this field. But I have never shipped anything out of country. My lack of export knowledge cause my stupidly took the Motorola document for the trip, I have no intention to break the law.

All to the best of my knowledge, the above statement is true and correct. The statement is voluntary, and it was made without threat, promise or coercion. I have agreed to consent to search my residence, 2331 County Farm Lane, Schaumburg, Illinois, 60194.

The statement was signed by Jin at 8:32 p.m. on March 1, 2007. (Tr. 142-44; Govt. Ex. HJ 1.)

64. In addition to consenting to a search of her residence, Jin also consented to a search of her computers. The search of her home occurred during the evening and early morning hours of March 1-2, 2007. (Tr. 145, 154-55.)

March 2, 2007

65. Jin was next interviewed by Agent Diekmann in her home on March 2, 2007. Her husband was also present, and they were both advised of their Miranda rights. During this interview, Jin was asked about Gengshan Liu (spelling provided by Jin). Jin said he was located in Beijing, and that she had met with him at least three times in Beijing: in April 2005, November 2005, and during her last trip to China, from November 2006 to February 2007. She said that Liu had given her his phone number in order to facilitate meetings with him whenever she was in Beijing. She said that the second meeting was similar to an interview, and that they discussed her work experience and technical expertise. (Tr. 146-48.)

66. During the third meeting, she and Liu discussed whether she could provide assistance on a short message project. Liu also asked her to review the Chinese-language documents found in Jin's possession on February 28, 2007, to determine how much assistance she could provide on the projects. She viewed this as a form of probation. Jin said that she

would work on the project and provide whatever she had done to him when she finished. She said that she told Liu that she had terminated her employment at Motorola. Jin also told Agent Diekmann that she had planned to meet with Liu in Beijing during her February 28th trip, and that she believed Liu was going to offer her employment at Sun Kaisens. (Tr. 148-50.)

67. On March 5, 2007, $115,000 was transferred from Jin and her husband's account in Chicago to a bank in China. (Govt. Ex. CHA 1.)

68. There was no mortgage on Jin's home in 2007. (Tr. 636.)

iDEN technology

69. Bruce Drawert, the government's expert witness regarding the technology at issue and the purported trade secrets, testified extensively regarding iDEN technology generally and the documents at issue in this case specifically. Although the Court finds that Drawert is clearly a "company man," his testimony was detailed and largely objective.

70. Drawert received his master's degree in mechanical engineering in 1983. He began working at Motorola in August 1991 as a digital signal processing engineer. In 1997, he became a system architect, a position he still holds today. He was also named a distinguished member of the technical staff. (Tr. 239-46.)

71. During his twenty-year career with Motorola, Drawert has principally worked on iDEN technology. When he first started with Motorola in 1991, iDEN technology was in its prototype stage. Drawert was part of the team responsible for inventing and developing iDEN at Motorola. Specifically, he was the co-developer of the iDEN base radio signal processing software. iDEN obtained its first customers in 1993. (Tr. 240-43, 309.)

72. Dr. Ray Nettleton testified as Jin's expert witness. Dr. Nettleton provided

professional and objective testimony, which the Court largely credits. Nevertheless, as discussed more specifically below, Dr. Nettleton's testimony tended to be general rather than specific, and some of his opinions were contrary to objective evidence.

73. Dr. Nettleton works in the field of wireless technology. He received a master's degree in electrical engineering and a Ph.D. from Purdue University. His thesis topic was CDMA for cellular communications, and he holds two patents in CDMA technology stemming from his thesis work. Dr. Nettleton has worked as a professor, a contractor for the military and NASA, for a technology company as director of wireless research, as a private consultant for clients including MCI and Motorola, and as a co-founder of a communications start-up company. He has published over 80 papers in the trade press, technical journals, and at conferences. (Tr. 674-77.)

74. Dr. Nettleton worked for a company contracting to Motorola in the 1990s in Beijing, China, and assessed an iDEN network that was being deployed in Beijing. Dr. Nettleton also evaluated iDEN technology for MCI in the early 1990s as it was coming on to the market, and the design of an iDEN system that was to be deployed in São Paolo, Brazil. (Tr. 677-78.)

Cellular Phone Technology

75. Cellular phone technology employs both open and proprietary standards. A standard is a set of documents or specifications that describe how the various elements in a network should behave and what functions they should perform. (Tr. 690.)

76. Open standards are available to any member of the public and can be downloaded from the Internet. The purpose of open standards is to ensure compatibility between the equipment of different manufacturers so that it works on the same network. Open standards are

maintained by committees made up of technical staff members of manufacturers and government regulators. The two main bodies are called 3GPP and 3GPP2. Open standards do not provide information on how to actually build a system, so manufacturers develop hardware and software that complies with the standard but that may not have similar features as other competitors' products that also comply with the standard. (Tr. 690-92.)

77. Proprietary standards are sets of documents or specifications like open standards, but which are held within a company or group of companies without publication. (Tr. 691.)

78. Cellular phone technology has evolved over time. Since cellular technology was first developed in the United States in the early 1980s, there have been four generations of technology. First generation ("1G") technology was analog and worked similarly to old radio telephones, with no possibility of significant data transmission. (Tr. 685-86.)

79. Around 1990, the first generation of digital cellular technology, known as second generation ("2G") technology, began evolving. 2G technology uses circuit-switch technology for voice and data, meaning channels are dedicated to individual calls, whether people are speaking or not, and when a user is in a data session, the radio signal is dedicated to that user. 2G technology employs digital voice, and the data rate available is around 64 kilobits, which is sufficient for text messaging and email. The most typical types of cell phone technology initially developed in the second generation were GSM and CDMA. GSM became a global standard, and billions of GSM units have been sold worldwide. CDMA stands for Code Division Multiple Access. CDMA was initially proprietary, but later became an open standard. (Tr. 674-75, 686-88, 696.)

80. By the 2000s, cellular technology had evolved into the third generation ("3G").

3G technology supports higher data rates, usually ones to tens of megabits per second, which permit the transmission of emails with attachments, complex web pages, and video. (Tr. 687.)

81. Currently, fourth generation ("4G") technology is being launched around the world. 4G technology has very high data rates, typically from 100 to 500 megabits per second. (Tr. 687.)

82. Both 3G and 4G technology use packet data, meaning that circuits or channels are not assigned in a dedicated way to any one user. Rather, packets, or a group of bits, are sent when needed and the same channel is available for other users. (Tr. 687.)

83. Each generation of technology takes around ten years to define and evolve. This means that at any given time, while the current generation is being deployed and used, the next generation is being developed. This leads to an overlap between the generations, as some people keep their older phones while others buy new ones. At some point, the older cellular technology is phased out completely to enable the newer technology to access the spectrum used by the older technology. (Tr. 688-89.)

iDEN

84. iDEN is a proprietary standard created by Motorola for cellular telecommunications technology. iDEN is 2G technology. Its top speed is 64 kilobits per second. iDEN does not use and is not compatible with CDMA. (Tr. 692-93.)

85. Most of iDEN is based on open standards. The unique aspect of iDEN is the air interface, which is the set of signals exchanged between the mobile unit and the base station. The other parts of the iDEN network resemble the GSM network, which is an open standard. (Tr. 693.)

86. iDEN was developed in response to a problem with a specific frequency band called Specialized Mobile Radio ("SMR"). The SMR band was originally envisioned as a specialized service for first responders and private businesses. As a result, individual groups of channels were assigned to individual companies or first responder services like the police. The channels were usually assigned in groups of four, but the four were not contiguous. This meant that when Fleet Call, later to become Nextel, began purchasing spectrum from the companies that owned the channels in order to aggregate spectrum, Fleet Call could not guarantee contiguous channels. As a result, GSM and CDMA could not be used because they required the aggregation of a large number of contiguous channels. The only alternative was to use individual channels one at a time, 25 kilohertz apart. iDEN was developed to address this need. (Tr. 692, 695-96.)

87. While the development of iDEN served as a solution to this problem, the use of the individual channels came with limitations. Specifically, the use of 25 kilohertz channels limits the data rate that can be achieved. iDEN efficiently uses the narrow space of individual channels, but it does not have the capabilities necessary to provide very large bandwidths. Dr. Nettleton opined that because it is not possible to aggregate adjacent channels to produce wider bandwidth with iDEN, there is no development path through which iDEN can achieve higher data rates, meaning it is at a technological "dead-end." iDEN cannot develop into 3G or 4G technology. (Tr. 697.)

88. iDEN is a turnkey system. This means that it has end-to-end network elements, including the subscriber unit, commonly known as the mobile device, as well as the infrastructure to support it. It also knits in with the Public Service Telephone Network, which means that its mobile devices can reach any other mobile device and/or landline. The major

infrastructure pieces of the iDEN network include the mobile switching center, the base station controller, base radios, an access controller gateway, packet data network elements including mobile data gateway and routers, and dispatch and application processors. (Tr. 241-42.)

89. iDEN customers are located globally. (Tr. 247.) iDEN was introduced in China in around 1995 or 1996. (Tr. 694.) iDEN customers offer services directly to consumers, also known as subscribers, and to enterprise. The services offered to subscribers are: (1) interconnect, which is regular telephone service; (2) dispatch, which is push-to-talk; (3) short message service, which is text messaging; (4) and packet data, which enables internet applications. (Tr. 247-48.) Competitors of Motorola provide similar features; it is the way that iDEN supports and provides these features that is unique. (Tr. 320.)

90. iDEN is best known for its push-to-talk feature. Unlike a telephone call, which is a full-duplex conversation from one handset to another, push-to-talk is a half duplex. This means that it is a walkie-talkie style of conversation. The conversation can be one to many, and only one person can talk at a time. The motivation behind push-to-talk systems was to enable members of a dispatch system, such as taxis and first responders, to talk instantly to another member or group of members of the same network. In 2007, several of iDEN's competitors provided push-to-talk features that rely on open standards, such as Tetra. iDEN's push-to-talk service is the fastest in the market, meaning it can achieve a call setup time in approximately 500 milliseconds. (Tr. 249-50, 317)

91. Technology that competes with iDEN includes CDMA, GSM, LTE, and Tetra. No company owns these technologies; rather, they are standards that are publicly accessible. iDEN, on the other hand, is proprietary technology that is not publicly accessible. (Tr. 264-65,

697-98.)

92. Another difference between iDEN and GSM and CDMA is, as previously mentioned, that an iDEN radio frequency channel is only 25 kilohertz wide. GSM technology requires a 200 kilohertz channel. CDMA requires a 1.25 megahertz channel. Due to the larger channels, GSM and CDMA are more efficient in terms of how many telephone users they can support per megahertz, and can carry data at much higher speeds than iDEN and other 2G technology. (Tr. 266-67, 696-988.)

93. Tetra is an open standard that has similar functionality as iDEN when it is used with 25-kilohertz channels. Unlike with iDEN, it is possible to use Tetra on accumulated adjacent channels to provide higher data rates. It also supports ground-to-air transmission, which iDEN cannot support. Tetra phones are also capable of communicating like walkie-talkies, without the need for an intermediate network. (Tr. 700-01.)

Value of iDEN

94. iDEN generates revenue for Motorola through hardware sales, software and licensing sales, and support and services. (Tr. 328-29.) The three main components of the iDEN system are the iDEN subscriber unit, the base station equipment, and the mobile switching center. All of these components contain iDEN software. Aside from RadioFrame, which manufactures certain base radios for iDEN pursuant to a nondisclosure agreement with Motorola, only Motorola manufactures iDEN software and hardware. (Tr. 327-28.)

95. When Motorola adds a new customer on an iDEN network, the customer must purchase most of the systems' components from Motorola, such as handsets, a certain number of base stations, and switching equipment. If an existing customer expands its coverage area, at a

minimum, it needs to buy more base radios. (Tr. 269-71.)

96. All but one of the components employed when the push-to-talk feature is used contain iDEN software, and Motorola sells the components. (Tr. 261-62.) While competing technologies use some of the same components as iDEN in transmitting a call, certain software related to the transmission path is unique to iDEN. (Tr. 255.) Motorola does not currently have any competitor in the iDEN market for iDEN components. (Tr. 289.)

97. As of February 2007, Motorola had over 700 employees related to iDEN, and there were 32 cellular phone operators using iDEN. The 32 operators were located in 22 countries worldwide. In 2007, several iDEN operators had service provider arrangements with government agencies. The Israeli Defense Forces subscribed to the iDEN system in 2007. (Tr. 334-36.)

98. Motorola monitors the number of iDEN subscriber units around the world. While the total number of iDEN subscribers is decreasing worldwide, outside the United States and Canada the total number of subscribers is increasing. As of July 2011, there were between 19 and 20 million iDEN subscribers. (Tr. 332-37.)

99. iDEN revenues decreased in 2006 compared to 2005. Motorola reported to the SEC in 2006 that it expected iDEN sales to decline further in 2007. Net sales of iDEN infrastructure equipment has also been declining since 2006. (Tr. 344-46.)

100. Dr. Nettleton testified that he "cannot imagine" why any other entities would want to build an iDEN system as of 2007 because an open standard that was more advanced than iDEN was available, and iDEN was already an obsolete generation of cellular technology. (Tr. 715.) As discussed in more detail below, Dr. Nettleton also opined that none of the charged trade

secret documents would have been of value to any entity outside of Motorola in 2007. This opinion was based on his belief that iDEN had been eclipsed technologically by 3G and 4G technology, and therefore that no one would be interested in developing an iDEN-like system or want to know anything about it. (Tr. 703-04.) While the Court finds that this belief is sincere on the part of Dr. Nettleton, the Court discounts his opinions regarding the value of iDEN generally and the trade secret documents specifically because these opinions are contradicted by the fact that the use of iDEN technology was expanding in certain parts of the world in 2007. The objective evidence before the Court indicated that—eclipsed or not by superior technology—iDEN still had growth potential in certain parts of the world in 2007. Although many consumers may want the latest technology, others are content with less expensive, less advanced options. Thus, while iDEN technology may be phased out and become obsolete in the long run, it was still a viable product that was generating revenue for Motorola in 2007.

The charged documents: Moto 1, Moto 2, and Moto 3

Moto 1

101. The first purported trade secret document, Moto 1, is titled "Harmony Support for Horizontal Dispatch Networking, SAD-172." Harmony is a small-scale iDEN system for customer sizes of about 50,000 subscribers. A typical customer for the Harmony system would be a company, an academic campus, or an entity of a similar size. (Tr. 272, 710; Govt. Ex. Moto 1.)

102. Moto 1 is marked as "Motorola Confidential Proprietary." The following statement is found on the cover of Moto 1: "The information contained in this document is classified Company Confidential. The use and divulgence of any part of this information can

seriously affect the welfare and financial security of the company." (Govt. Ex. Moto 1.)

103. Moto 1 is a systems architecture document, which means that its intended audience is iDEN network element developers and software coders. Systems architecture documents are teaching instruments. Moto 1 was created on June 17, 2005, and it was last revised on August 30, 2006. (Govt. Ex. Moto 1, at ii; Tr. 272-75.)

104. Moto 1 discusses the horizontal dispatch networking feature of Harmony, which involves connecting one urban area to another in order to enable push-to-talk between those areas. Without this feature, a user would be limited to using push-to-talk through the local Harmony switching center, meaning the user could not use push-to-talk on a nationwide basis. (Tr. 272-73.) Moto 1 discusses the changes that have to be made to the Harmony system to support horizontal dispatching. (Tr. 711.) Moto 1 describes only part of iDEN, not the whole system. (Tr. 277.)

105. Moto 1 contains information that describes aspects of how the user's voice is conveyed over the internet protocol. Specifically, this information relates to the interconnection of hDACs. The hDAC is a piece of hardware containing iDEN-specific software that is one of the central network elements of the horizontal dispatch networking feature. Table 2 on page 29 of Moto 1 contains numbers to which a system format must adhere in order to enable the interconnection. The numbers convey how the audio moves from one point to another. This is a feature unique to iDEN, and it is used wherever the horizontal networking feature is deployed, which is globally. (Tr. 276-82.)

106. While some of the information in Moto 1 is shared with customers, the information related to the formatting of the voice as it traverses the internet protocol and the

interconnection of the hDACs has not been shared.

107. The information in Table 2 could benefit someone outside of Motorola because it is part of the information necessary to build a competing iDEN product that performs the same functions, and it could also be used as a part of discovering the content of the voice that appears on the network. (Tr. 278-29, 282.)

108. In making this finding, the Court acknowledges Dr. Nettleton's opinion that Moto 1 would not have been useful to anyone outside of Motorola. He based his opinion, first, on his belief regarding the value of iDEN technology generally. As discussed above, however, the Court believes this opinion is contradicted by the objective evidence regarding iDEN revenue in 2007.

109. Dr. Nettleton also highlighted several problems with Moto 1 as a document. Specifically, he pointed out that Moto 1 is a delta document, which means that it only refers to the changes that have to be made to other documents in order to realize the horizontal dispatching capability. Thus, it does not describe the system itself, only the changes. Moto 1 also uses multiple abbreviations that are Motorola-specific and necessary to understand the document. There are also deletions, edits, and additions in the document that make clear that it is not a final document reflective of the final design of the feature. (Tr. 712-13.) While Dr. Nettleton's testimony regarding the general problems with Moto 1 as a document is clearly supported by the document itself, none of these problems contradict Drawert's very specific testimony regarding the value or usefulness of the information related to the formatting of the voice as it traverses the internet protocol found in Table 2 of Moto 1. Of course, that information would be *more* useful if the document were not in draft form, did not contain abbreviations, and

explained the whole Harmony system, as opposed to just changes to that system necessary to enable the horizontal dispatching feature. That the document is not in an optimal state, however, does not mean that the accurate information in Table 2—information that would be necessary to build a competing product—would not be "useful" or "valuable" to someone outside of Motorola.

Moto 2

110. Moto 2 is the second charged trade secret document. It is entitled "iDEN EOTD-based 911 Location without HAMR." (Tr. 283; Govt. Ex. Moto 2.) Moto 2 is marked as "Motorola Confidential Proprietary." It was created on March 30, 2000, and last revised on November 14, 2000. Drawert is one of the authors of this document. (Tr. 287, 316.) The following statement is found on the cover of Moto 2: "The information contained in this document is classified Company Confidential. The use and divulgence of any part of this information can seriously affect the welfare and financial security of the company." (Govt. Ex. Moto 2.)

111. Moto 2 is a white paper. A white paper is used by developers to estimate how many staff months would be required to put a particular feature together after an investigation is done on that feature. White papers also illustrate whether a particular feature was successful in meeting an intended goal. The intended audience of a white paper within Motorola is an iDEN network developer or a network element developer. (Tr. 283-84.)

112. Moto 2 discusses the feature known as "iDEN EOTD-based E911 location." E-OTD is a type of technology that may be used to establish the location of a cell phone. This location technology was explored by iDEN developers in response to the FCC's enhanced 911

mandate. In 2000, when Moto 2 was created and last revised, the mandate required that with two-thirds of calls, the phones should be locatable within 50 meters, and that with 95% of calls, the location of the phone should be accurate within 150 meters. (Tr. 284, 705-06.)

113. The feature discussed in Moto 2 was not implemented in its entirety in iDEN. Some of the information was implemented, including information indicating performance, timing specifications, and channel structures for the base station control channel. Figure 3 on page 20 of Moto 2 contains information that illustrates the channel structure, or how the iDEN system uses its broadcast control channel. iDEN, or any other cellular technology, cannot function without a broadcast control channel. The broadcast control channel set forth in Figure 3 is specific to iDEN. It contains numbers and sizes related to the broadcast control channel used in iDEN. The described broadcast control channel structure is in continuous use in iDEN technology, and is found in every iDEN product. (Tr. 290-94.)

114. Some of the information in Moto 2 has been shared with customers and, pursuant to a nondisclosure agreement, with Radioframe, the company that built base radios for iDEN. The information in Figure 3 is only disclosed under a nondisclosure agreement. (Tr. 285, 294.)

115. The information in Figure 3 would be valuable to someone outside of Motorola because it is part of the information would be necessary to build a competitive base radio. It would also be useful for someone who is interested in understanding how to get information off the radio frequency; while Figure 3 does not provide all of the information necessary, it does detail necessary pieces. Without this information, an iDEN-based radio would not function on an iDEN network. (Tr. 289, 296.)

116. Dr. Nettleton opined that Moto 2 would have been useless to anyone outside or

inside of Motorola in 2007 because, first, by 2007, all cellular providers had given up on E-OTD as a possibility for location technology as it turned out to be quite inaccurate and difficult to implement. Second, better technologies, including GPS, were adopted as early as 2002, and by 2004 in the case of Motorola. Third, E-OTD technology was an open standard available to the public as early as 2000. Finally, the document itself indicates that it would not have fulfilled the FCC's requirements. (Tr. 706-11.) Once again, although the Court does not doubt these general facts regarding E-OTD, they do not impact the Court's finding that the specific information identified by Drawert in Figure 3 could be useful to a potential competitor. Although E-OTD was abandoned by Motorola by 2004, the information pertaining to the base station channel control structure in Figure 3 was implemented in iDEN technology, and is in continuous use today.

Moto 3

117. The third charged trade secret, Moto 3, is entitled "Base State System MOBIS Call Processing Interface Specification." (Govt. Ex. Moto 3; Tr. 296.) Moto 3 discusses the messaging protocol that is used between the access controller gateway and the base station controller in an iDEN system. MOBIS is a modification of the ABIS interface, which is the open standard interface switch over which communications between the base station and the rest of the network occur. Moto 3 was created on May 14, 2001, and was last revised on February 8, 2007. (Govt. Ex. Moto 3 at I-ii; Tr. 296-99, 713-14.)

118. Moto 3 is an interface control document. Interface control documents are used at Motorola to catalog messages that are used between network elements, and in this case, the base station controller and the access control gateway. The intended audience of Moto 3 is the

developers of the base station controller and the access controller gateway at Motorola. (Tr. 296-97.)

119. Moto 3 is marked as "Motorola Confidential Proprietary" in small font on the bottom of the pages of the document beginning with page "iii." The cover and the table of contents of Moto 3 are not marked as "Motorola Confidential Proprietary." (Govt. Ex. Moto 3.)

120. Moto 3 contains 143 tables, each of which illustrates a message within iDEN technology. Moto 3 also has 29 figures that set out engineering information related to general procedures in iDEN. Table 119 on page 111 provides a decoder to all the messaging used on the protocol. The table consists of three columns. The first column provides the values that identify the message type; the second column, the definition column, describes the purpose of the message; and the last column directs the reader to the appropriate section of the document for further detail on the given message. (Tr. 297-303.)

121. Moto 3 has not been shared with anyone outside of Motorola because the two network elements that use this information, the access controller gateway and the base station controller, are exclusively made by Motorola. (Tr. 300-01.)

122. The information contained in Table 119 would be valuable to someone outside of Motorola because it would be necessary to build a competing base station controller or access controller gateway. The information in Table 119 could also be used to intercept messages in the iDEN network. (Tr. 303.)

123. Dr. Nettleton opined that Moto 3 would not have been useful to an entity outside of Motorola because, first, although MOBIS is a modification of ABIS that suits Motorola's own design objectives, it still conforms with open standards specifications. Second, Motorola has

disclosed general information regarding how MOBIS works in training courses. Finally, the information in Moto 3 refers to specific messages that need to be sent that accommodate the specific air interface that iDEN uses; thus, anyone developing any other kind of system would not find the information useful. (Tr. 713-15.) The Court discounts Dr. Nettleton's ultimate opinion, first, because it relies upon his assumption that iDEN is worthless technology. Second, aside from his ultimate conclusion and his belief in the obsolescence of iDEN, none of his testimony contradicted Drawert's testimony that someone seeking to build a competing iDEN base station would find the information in Table 119 valuable. Additionally, that Motorola may have disclosed general information regarding MOBIS outside of Motorola does not contradict Drawert's testimony that the very specific information in Table 119 has not been shared.

Motorola's security measures

Physical security

124. In February 2007, there were 40 security employees on the Motorola campus working as console operators, patrol officers, and security officers. Console operators monitor the security cameras, alarms, the access system, and the emergency line, and dispatch patrol and security officers as needed. Patrol officers drive around the campus and conduct foot patrols in each of the campus buildings. Security officers also guard the points of entry of the campus buildings. (Tr. 370-72.)

125. The Motorola campus has four gates through which cars can enter. The gates are opened by an access card or by a security console operator. (Tr. 372.)

126. Once a person gains access to the campus, that person must present an access card in order to enter a building. Motorola employees are only given access to the buildings in which

they work unless they have manager approval for additional buildings. (Tr. 379.)

127. All of Motorola's doors are monitored by security cameras. Some doors are guarded by security officers. Doors that do not have security guards require an access card for entry, and because they are revolving doors, they only permit one person to enter at a time. (Tr. 379-82.)

128. Security officers are not required to look through every bag that employees remove from the building because Motorola does not have enough security officers to accomplish that task. According to Catherine Hall, Motorola's security operations supervisor, it is not Motorola's policy to "search" bags. Instead, "most employees" know that they should unzip and open any bags or briefcases to show the security officers the contents before they leave the building. (Tr. 387-88, 391.)

129. Security camera footage from the night of February 26-27, 2007, shows Jin carrying two bags past security without being stopped. The footage shows Jin reentering the building, and then leaving again with her arms full of papers and binders through a door that the security officer held open for her. (Tr. 394, 397.)

POPI

130. POPI is the name used to describe Motorola's program "Protecting Our Proprietary Information." At the orientation of new hires, Motorola's security operations supervisor informs new hires about POPI, explains the information classification system to them, and informs them of Motorola's "clean desk policy," meaning that employees are required to secure all confidential proprietary information when they leave at night. (Tr. 367-69.)

131. Motorola's security team conducted POPI audits in 2007. During POPI audits,

the POPI team conducted random audits of employees' work areas to ensure that they had not left proprietary information laying on their desks or in unlocked cabinets. In February 2007, POPI audits were performed two to three times a week. Motorola also had POPI bins for proprietary information that was discarded. (Tr. 369-70.)

132. In addition to providing procedures related to the physical security of proprietary information, the POPI policy also described the classification scheme within Motorola and how Motorola employees should protect the information based on its level of classification. Motorola employees were informed of this policy when they were hired, during an annual refresher training, and during POPI audits. (Tr. 435-36.)

133. Every document added to Compass was given a data classification by its author. The data classifications were based on the sensitivity level of the data. The four classifications were "General Business Information," "Motorola Internal Use Only," "Motorola Confidential and Proprietary," and "Motorola Registered Secret Proprietary." According to the POPI policy, "Motorola Confidential Proprietary" data is that which an unauthorized disclosure of would cause "substantial detrimental effect." Examples are personnel information, some financial data, and certain technical information. "Motorola Registered Secret Proprietary" data is that which an unauthorized disclosure of would cause "serious damage." The listed examples are trade secret data, new product development, new process development, certain financial and planning data, and long range or strategic planning. According to the POPI handbook, Motorola employees were only supposed to take classified data off of Motorola premises with the required approval. (Govt. Ex. Air 17 at 7; Tr. 435-36.) The three charged trade secret documents were classified as "Motorola Confidential Proprietary."

Computer and network security

134. Thomas Chmielarski, currently the threat team manager at Honeywell and formerly at Motorola for eight years, testified about Motorola's computer security measures. Chmielarski began on the technical team in Motorola Information Protection Services in 2000. At some point around the end of 2004 or early 2005, Chmielarski transitioned to a team called the Motorola Wireless Security Services, which performs security services for Motorola and Motorola customers. In this role, Chmielarski's primary responsibility was to design, build, and operate a Security Operations Center that monitored Motorola systems 24 hours a day, seven days a week. The professionals at the Security Operations Center monitor access to the Motorola network, network traffic, and other information being logged, looking for anomalous behavior. (Tr. 411-14, 475-76.)

135. In 2007, Chmielarski began working as a senior forensic investigator for Motorola. In this role, he investigated Motorola employees suspected of inappropriate use of computer resources. (Tr. 415-17.)

136. The Motorola network or intranet is the term used to describe all of the various systems that enable the business functions of Motorola, such as file servers, email servers, collaboration servers, and the infrastructure that allows Motorola employees remote access to the network. Only Motorola employees, consultants, and contractors have access to the Motorola intranet. (Tr. 420.)

137. The first component of the Motorola computer network as it existed in February 2007 consisted of users with computers. In order to access the Motorola network, each computer had its own individual safeguard, such as requiring a user name and password to log on.

Passwords were required to be a certain length, a combination of uppercase and lowercase letters, numbers, or special characters, and changed regularly. (Tr. 418-19, 422-23.)

138. Once a person logged onto the Motorola network, a log-on banner would appear informing the user that it was a Motorola asset for authorized use only and that any use of the system was subject to monitoring. (Tr. 424.)

139. A user's access to the Motorola network would vary depending on the access granted to the user's account. For example, access to individual file servers was governed by each department or group that set up the file server. (Tr. 424-25.)

140. On some computer systems, there was disk-based encryption that prevented a person from loading and viewing the contents of the hard drive without the encryption password. Motorola also used anti-virus software on the computers. (Tr. 418.)

141. In addition to the end user security measures, the Motorola computer network had the Motorola perimeter, which is two layers of firewalls that protect Motorola from non-Motorola networks. There were also internal intrusion detection systems that identified anything unusual occurring across the network. (Tr. 419-20.)

142. Compass is Motorola's main web-based collaboration tool used by the entire company. (Tr. 425, 431.) Motorola employees use Compass to share documents, calendar items, project plans, meeting minutes, and everything necessary to facilitate cooperation between departments or groups around the world. It is organized as a folder system. In 2007, all Motorola employees had some level of access to the general business documents on Compass. For specific folders and files, however, an employee must have been granted access to it. The person responsible for granting access to a particular file or folder was typically the document

owner. (Tr. 432-34.) While Motorola maintained records of who accessed each document on Compass, the Security Operations Center did not actively monitor Compass. (Tr. 437, 480.) In February 2007, there was no systems of alarms that would be triggered by excessive downloading in Compass because there would be too many false positives. (Tr. 494.)

143. VPN stands for Virtual Private Network. Motorola's VPN is known as MVP. (Tr. 421.) The VPN enabled employees to remotely access Motorola's network. Only employees with a "business need" were granted permission to use the VPN. Access to VPN required a combination of credentials and software. (Tr. 437-38.)

144. There are certain measures that can improve a company's security that Motorola did not employ. For example, to address the security challenges presented by USB devices, which are small devices that can hold a large amount of data, companies can disable all USB ports, selectively enable the USB ports with third party software, or monitor USB traffic with software. (Tr. 466-70.) Another fundamental protective measure for companies is to deactivate a user account when the user leaves his or her job. It is also recommended that a company reassess a user's access when the user changes roles within the company. A company's risk can also be lowered by regularly reviewing access lists and determining whether the access permissions are appropriate. (Tr. 470-72.)

145. Jin had access to MVP and Compass throughout her time at Motorola, including while on medical leave. Jin accessed the Motorola network remotely 40 times in 2006, including from a Lemko computer. (Tr. 486-90.) Jin also extracted more than a thousand documents from Compass, the majority of which occurred during a short amount of time. Many of the items Jin downloaded were outside the scope of her employment and pertained to projects outside of her

area, including Tetra. (Tr. 493-94.) The charged documents, however, were within Jin's project area.

Code of conduct and computer resource policy

146. In addition to the measures described above, it is also the responsibility of Motorola employees to safeguard Motorola's proprietary information. (Tr. 388.) This is made clear to Motorola employees through the Motorola Employment Agreement, the Code of Conduct, and the policy on the Appropriate Use of Computer Resources.

147. On the date she began working at Motorola, Jin signed the Motorola Employment Agreement, the Code of Conduct Understanding, and the policy on Appropriate Use of Computer Resources. (Govt. Ex. MBR 3; Tr. 351.)

148. Pursuant to the Employment Agreement, Jin agreed "[n]ot to use, or to publish, or to otherwise disclose to others, either during or subsequent to my employment by Motorola, any confidential information of Motorola . . . except as my Motorola duties may require." (Govt. Ex. MBR 3; Tr. 351-52.) She also agreed that upon termination of her employment by Motorola, she would "promptly deliver to a designated Motorola representative all documents and other records which relate to the business activities of Motorola, or any other materials which belong to Motorola." (Govt. Ex. MBR 3.)

149. Jin also affirmed her compliance with the Code of Conduct, which provides that "[a] Motorola employee may not disclose confidential Motorola information to any person other than in the proper discharge of the employee's Motorola duties." (Govt. Ex. MBR 4; Tr. 353-54.)

Chinese Military Industrial Complex

150. Shawn Bateman, who spent over fifteen years in the Air Force and the Defense Intelligence Agency studying the Chinese military, testified as an expert for the government regarding the Chinese Military Industrial Complex. (Tr. 552.) Her testimony was thorough, objective, and credible.

151. Most industrialized countries have a military industrial complex. (Tr. 585.) Military industrial complexes seek to improve the country's military weaponry, training, and communications, among other things, through a collaboration between governments, militaries, and private industries, often referred to as defense contractors. (Tr. 587.) One of the primary differences between the military industrial complexes in China and the U.S. is that in China, the leadership of many of the different entities have been appointed by the state and many of the entities have been heavily funded by the state. (Tr. 590.)

152. In approximately 2007, the chief concern of the Chinese military was modernizing to achieve a level of technological parity with the United States. The Chinese military's primary focus was to improve the Chinese economy, and as the economy improved, the technological capabilities that were being introduced would be incorporated into the military modernization. Dual-use technology was particularly valuable because it could be applied to both commercial and military applications. China sought to obtain dual-use technology from companies in all modern countries, but the United States was a major focus. (Tr. 556-57.)

153. The Chinese Military Industrial Complex is a conglomeration of military and commercial enterprises, factories, research institutes, and decision-making bodies. (Tr. 538.) The structure of the Chinese Military Industrial Complex is headed by the Communist Party, the ruling government entity. Below the Communist party is the Chinese Military Commission, the

Chinese military leadership, which is directed and guided by the Communist Party. The chairman of the Communist Party is also the chairman of the Chinese Military Commission. (Tr. 554-55.)

154. There are four major departments under the Chinese Military Commission: the General Logistics Department, the General Political Department, the General Armaments Department, and the General Staff Department. These departments have oversight of the armed forces, the PLA Navy, Air Force, and Second Artillery. (Tr. 555, 558-59.)

155. The General Staff Department is responsible for the overall operations of the military. (Tr. 558.) It has seven major departments, including the Communications Department, which oversees, develops, and maintains the command-and-control infrastructure of the PLA. The command-and-control infrastructure is composed of the radios, telephones, fiber optics, and other technology that facilitates the communication between military entities at different levels during the prosecution of a conflict. (Tr. 560-61.)

156. The Communications Department oversees several entities, including the Chongqing Communications Institute. The Chongqing Institute is a major training institute that provides trained personnel and knowledge acquired from its interactions with civilian universities and research institutes to the communications entities across the PLA. The Chongqing University of Posts and Telecommunications works with the Chongqing Communications Institute. (Tr. 562-63.)

157. The 61st Research Institute is another entity under the General Staff Department. It focuses on the research and development of command-and-control equipment and command automation that is integrated into the overall command-and-control infrastructure of the PLA.

(Tr. 564.)

158. Factory 6905 produces some of the components developed by the 61st Research Institute. Factory 6905 is also called the Chongqing Weihua Electronics Factory. The use of two names results from the Chinese military's efforts in the 1970s and 1980s to use military capabilities to develop civilian factories. This process led to the naming of the numbered military institutes by civilian commercial names as well. The result is that two entities that appear to be different, are, in fact, the same entity. (Tr. 564-65.)

159. The General Staff Department also works with commercial organizations in China to ensure that the Department has the necessary technology to create and maintain the command-and-control structure. (Tr. 561-62.)

160. On the civilian side, the highest governing body under the Communist Party is the State Council. (Tr. 555-56.) It has approximately equal power and influence as the Chinese Military Commission. Like the Chinese military, the State Council is filled with appointed Communist party members. The State Council also has its own role in directing the modernization of China's defense industry that supplements and works in conjunction with the Chinese military's goals. (Tr. 566.)

161. The State Council oversees several ministries, including the Ministry of Information Industry. The Ministry of Information Industry is responsible for advancing the telecommunications capabilities of China and guiding the acquisition of technology to achieve that goal. This benefits the Chinese military because the technology that is acquired in a civilian capacity is directly accessible to the military. (Tr. 566-67.)

162. Within the Ministry of Information Industry is the China Electronics Technology

Group Corporation. This is one of the largest group corporations in China; it has 46 state-owned enterprises, 46 research institutes, 26 factories, and many subsidiary enterprises. The purpose of the China Electronics Technology Group Corporation is to develop communications capabilities in China. This development is valuable both commercially and to the Chinese military. (Tr. 567-68.)

163. The research institutes within the China Electronics Technology Group Corporation have both numbered and commercial names. The 7th Research Institute focuses on mobile communications and wireless capabilities. The 7th Research Institute works in conjunction with the research institutes on the military side under the General Staff Department, sharing technology and completing projects for the military. The 30th Research Institute focuses on cyber technology. This includes wireless security and secure communications for commercial and military applications. (Tr. 568-69.)

Documents found in Jin's possession

164. The documents admitted into evidence were found in Jin's possession in hard copy form on February 28, 2007, on Jin's laptop and portable electronic storage devices she had on February 28, 2007, and in Jin's residence on March 1, 2007. They include Motorola documents, including Moto 1, Moto 2, and Moto 3, documents in Chinese related to the Chinese military or Sun Kaisens, and personal documents.

Chinese Military Documents

165. The Chinese military documents found in Jin's possession clearly establish that Sun Kaisens develops telecommunications technology for the Chinese military, and that Jin had worked on such projects in the past. Several of the documents were authored by Chinese military

entities, or entities associated with the Chinese military, such as the Chongqing Communications Institute (Govt. Exs. Air 10 TR, THD 2 TR), Institute No. 61 (Govt. Exs. Air 18 TR, Air 19 TR, Ion 5 TR), the Ministry of Information Industry Data Communication Science and Technology Institute (Govt. Ex. Air 24), the No. 7 Research Institute of the China Electronic Technology Group (Govt. Ex. ION 4 TR), and the Communications Department General Staff Headquarters (Govt. Exs. THD 5 TR, THD 7 TR). Many of these documents were marked as classified "secret." (Govt. Exs. Air 18 TR, Air 19 TR, Air 24, ION 4 TR, THD 5 TR, THD 6 TR, THD 7 TR.)

166. The documents authored by the entities associated with the Chinese military address various aspects of the future Chinese military communications system, including specifications of what the military required in the next set of technological developments. (Tr. 716.) The documents indicate that telecommunications systems that were already available to the Chinese military and the requirements for future systems all required capabilities that iDEN could not provide. (Tr. 718.) For example, the Chinese military documents largely focus on CDMA, which is not compatible with iDEN. (Tr. 722; Govt. Exs. Air 18 TR, Air 19 TR, AIR 24 TR, ION 5 TR.) The telecommunications systems described in the documents also require much higher data rates than iDEN could support. (Tr. 722.)

167. One classified military document also discusses several technical requirements that could not be met using iDEN technology, such as accommodating anti-jamming, ground and air networking, supporting relaying and walkie-talkie mode with direct transmission from one mobile to another, and supporting frequency hopping multiple access. Each of these requirements disqualifies iDEN as a candidate for the communications system described in the

document. (Tr. 727-28; Def.'s Ex. 19.)

168. The documents also indicate a preference for soft switching over conventional switching because it is field portable. iDEN was using conventional switching as of 2007, although one component of iDEN has soft-switching capabilities. (Tr. 721-22, 749.)

169. Another document dated January 2007 contains a presentation entitled "An Introduction to Mobile Communication in Military Applications." The topics of the presentation are the current status of Chinese military mobile communication development, the demand for more development, learning from foreign military mobile communications development, and ideas for future development. In the section "Foreign Military's Mobile Communication Development Experience," the slide lists the "U.S. Military's Global Mobile Information System," "NATO's Trunked Mobile Communication System," "Israel's Secure Cellular Phone Applications," and "Ericsson's QUICKLINK Tactical Mobile System." The presentation also states that "[m]odern commercial mobile communications is developing rapidly. System capabilities are constantly improving. China's domestic GSM and CDMA mobile communication networks are increasingly efficient. China has been keeping abreast with developed countries in 3G and 4G development." (Govt. Ex. THD 2 TR.)

170. Two Chinese military documents found in Jin's possession mention telecommunications systems utilizing a channel width of 50 kilohertz. (Govt. Exs. ION 1 TR at 67; THD 3 TR at 8.) One document describes a system that uses a channel width of 25 kilohertz. (Govt. Ex. THD 1 TR at 12.)

Sun Kaisens Documents

171. Other documents in Chinese found in Jin's possession were authored by or relevant to Sun Kaisens. These documents indicate that Sun Kaisens works closely with the Chinese Military. (Govt. Exs. ION 3 TR, ION 7 TR, ION 8 TR, ION 9 TR, Air 23 TR.)

172. One document, a summary from the "Comprehensive Military Communications System 2nd General Meeting" organized by the 61st Institute, lists Sun Kaisens as a member of the General Assembly, "the highest decision-making body of the Comprehensive Mobile Communications Project." (Govt. Ex. ION 3 TR.)

173. The documents also demonstrate that Jin had done work for Sun Kaisens. One document labeled "Company Directory" lists Jin, as well as "Qi Shiqing," as General Manager, and "Liu Gengshan" under General Department. (Govt. Ex. Air 15 TR.) Although the document does not state that it is a Sun Kaisens company directory, the departments and listed employees indicate that it is from Sun Kaisens. Another document found in hard copy and on a hard drive, "Motorized Mobile Communication System Configuration Management System Project Request," lists Jin and Gengshan Liu as chief directors for the project. (Govt. Exs. Air 22 TR, ION 6 TR.)

174. The Sun Kaisens documents indicate that Sun Kaisens was focusing on technology related to soft-switching and CDMA. (Tr. 729.) The documents also indicate that the technology available to Sun Kaisens was more advanced than iDEN technology. (Tr. 732.)

Miscellaneous Documents

175. One document found in Jin's possession compares the digital trunk systems available in China. It appears to be an industry news article, and states that in 2000, the "Ministry of Information Industry officially issued the industry recommended standards, digital

trunk mobile communication system standards, which confirmed to trunk communication standards mainly based on the international standard TETRA, Standard A, and Motorola's U.S.A. standard iDEN, Standard B." The document also states that "Motorola is the sole manufacturer of iDEN whose interface is confidential, resulting in Motorola being the sole provider of iDEN networks. The costs for system equipment network setup and terminals are all high. Although iDEN development achieved a head start, its technology, while mature, obviously is not fit for the expansion of new business services." (Govt. Ex. ION 11 TR.)

176. Jin was also found in possession of a catalog produced by Thales, which is a catalog of military technology products. (Govt. Ex. AIR 27.)

CONCLUSIONS OF LAW

1. The EEA criminalizes two principal categories of trade secret misappropriation, "economic espionage" as defined by 18 U.S.C. § 1831, and "theft of trade secrets" as defined by 18 U.S.C. § 1832. Jin has been charged with three counts under each section.

2. Section 1832(a)(3), the theft of trade secrets provision, provides:

> (a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization . . . shall . . . be fined under this title or imprisoned not more than 10 years, or both.

18 U.S.C. § 1832(a)(3). In order to prove a violation of the theft of trade secrets provision of the EEA in this case, the Government must prove beyond a reasonable doubt that: (1) the information at issue—Moto 1, Moto 2, and Moto 3—were trade secrets; (2) Jin knowingly possessed the trade secrets; (3) Jin knew the trade secret information was stolen or

appropriated, obtained, or converted without authorization; (4) Jin intended to convert the trade secrets to the economic benefit of anyone other than Motorola; (5) Jin intended or knew that the offense would injure Motorola; and (6) the trade secrets were related to a product placed in interstate or foreign commerce. *Id.*

3. Section 1831(a)(3), the economic espionage provision, provides:

> (a) Whoever, intending or knowing that the offense will benefit any foreign Government, foreign instrumentality, or foreign agent, knowingly . . . (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization. . . shall . . . be fined not more than $500,000 or imprisoned not more than 15 years, or both.

18 U.S.C. § 1831(a)(3). In order to establish a violation of Section 1831(a)(3) in this case, the Government must prove beyond a reasonable doubt that: (1) the information at issue—Moto 1, Moto 2, and Moto 3—were trade secrets; (2) Jin knowingly possessed the trade secrets; (3) Jin knew the trade secrets were "stolen or appropriated, obtained, or converted without authorization"; and (4) Jin intended or knew that the offense would benefit "any foreign Government, foreign instrumentality, or foreign agent[.]" *Id.*

The Court will first analyze whether the Government met its burden in proving the first three elements common to Sections 1831(a)(3) and 1832(a)(3), and will then turn to the remaining elements under each section.

Elements Common to Sections 1831(a)(3) and 1832(a)(3)

Whether Moto 1, Moto 2, and Moto 3 were trade secrets

4. A threshold question under both sections of the EEA is whether each charged document qualifies as a trade secret. As an initial matter, instead of merely "point[ing] to broad areas of technology and assert[ing] that something there must have been secret[,]" *Composite*

Marine Propellers, Inc. v. Van Der Woude, 962 F.2d 1263, 1266 (7th Cir. 1992), the Government highlighted specific information in each document related to the technology at issue that qualifies as trade secrets. In Moto 1, the Government pointed to information contained in Table 2 on page 29 of the document relating to hDACs, hardware with iDEN-specific software, and the process by which audio is conveyed over the iDEN internet protocol through the interconnection of hDACs. Regarding Moto 2, the Government focused on the information about the iDEN base radio channel control structure found in Figure 3 of the document. In Moto 3, the Government pointed to the information that illustrates the decoding of messages used within the iDEN protocol found in Table 119 of the document. Consequently, the Court's analysis will focus on these specific areas of information in determining whether Moto 1, Moto 2, and Moto 3 qualify as trade secrets.

5. The EEA defines a trade secret as:

> [A]ll forms and types of financial, business, scientific, technical, economic, or engineering information . . . whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public[.]

18 U.S.C. § 1839(3). Thus, the Government must have proven the following elements as to each of the three documents at issue in this case: "(1) that the information [in the charged documents] [was] actually secret because it [was] neither known to, nor readily ascertainable by, the public; (2) that [Motorola] took reasonable measures to maintain that secrecy; and (3) that independent economic value derived from that secrecy." *See United States v. Chung*, 659 F.3d 815, 824-25 (9th Cir. 2011). Whether information qualifies as a trade secret is a fact-specific inquiry that

"requires an ad hoc evaluation of all the surrounding circumstances." *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 725 (7th Cir. 2003) (interpreting the Illinois Trade Secrets Act, which is based on the Uniform Trade Secrets Act ("UTSA")).[3]

Not known or readily ascertainable

6. Regarding the first element of a trade secret, whether the information is "not known to" or "readily ascertainable through proper means by the public," the Seventh Circuit has noted that there is some dispute as to whom "the public" includes. *See United States v. Lange*, 312 F.3d 263, 266-67 (7th Cir. 2002). While the Third Circuit assumed that "general" belongs in front of "public" in *United States v. Hsu*, 155 F.3d 189, 196 (3d Cir. 1998), the Seventh Circuit has suggested that "public" could just as plausibly be implicitly preceded by "educated" or "economically important." *Lange*, 312 F.3d at 266-67 (noting that "the public" could be shorthand for the longer phrase found in the UTSA of all "persons who can obtain economic value from its disclosure or use"). In *Lange*, the Seventh Circuit also observed that the phrase "readily ascertainable" can be "understood to concentrate attention on either potential users of the information, or proxies for them (which is to say, persons who have the same ability to 'ascertain' the information)." *Id.* at 268. Ultimately, the Seventh Circuit declined to decide whether "general" precedes "public" because even if it did, the information at issue in the case

[3] As the Ninth Circuit recently noted, the case law interpreting the EEA's definition of a trade secret is sparse. *Chung*, 659 F.3d at 825. Because the definition of a trade secret found in Section 1839(3) was derived from the UTSA, a model statute for civil actions for the misappropriation of trade secrets that many states have adopted, the Ninth Circuit considered instructive interpretations of state laws that have adopted the UTSA definition without substantial modification. *Id.* Although there are some differences between the definitions of a trade secret found in the UTSA and the EEA, the Court also considers cases that have interpreted the requirements for a trade secret under state law based on the UTSA.

before it was not "'readily ascertainable' to the general public, the educated public, the economically relevant public, or any sensible proxy for these groups." *Id.*

7. The Court concludes that the Government proved beyond a reasonable doubt that the information in the charged documents was "not known" or "readily ascertainable" to the public, whether defined as the general public or the economically relevant public. Regarding Moto 1, although some of the information in the document has been disclosed to customers, certain technical information has not been shared outside of Motorola. In particular, the technical information relating to the formatting of the voice as it traverses that internet protocol and the interconnection of hDACs has not been disclosed outside of Motorola. Thus, even though certain information in Moto 1 has been disclosed, Moto 1 still contains information—specifically the information about the hDACs on page 29 of the document—that was secret. *See Chung*, 659 F.3d at 826-27 (noting that while certain information in the purported trade secret documents had been disclosed at a conference, portions of the document had not been disclosed and thus the documents contained secret information).

8. Similarly, with Moto 2, certain technical information found in the document has been disclosed to customers and RadioFrame. Importantly, though, the information in Figure 3 about the iDEN broadcast control channel structure has only been shared pursuant to a nondisclosure agreement, which does not forfeit trade secret protection. *Rockwell Graphic Sys.*, 925 F.2d at 178. As for Moto 3, the information in Table 119 that decodes the messages used in the iDEN protocol has never been shared outside of Motorola. Accordingly, the relevant sections in Moto 1, Moto 2, and Moto 3 meet the first element of a trade secret.

Reasonable measures to maintain secrecy

9. Under the second element of a trade secret, whether the precautionary steps taken by the owner of the purported trade secret were reasonable, the Court must balance "the costs and benefits" of a given precautionary measure, which will "vary from case to case." *Rockwell Graphic Sys. v. DEV Indust.*, 925 F.2d 174, 179 (7th Cir. 1991) (interpreting Illinois law). On the one hand, failure to take steps to protect a secret "is persuasive evidence that the secret has no real value" and is undeserving of the law's protection. *BondPro Corp. v. Siemens Power Generation, Inc.*, 463 F.3d 702, 708 (7th Cir. 2006) (interpreting Wisconsin law). Additionally, "[i]f the owner fails to attempt to safeguard his or her proprietary information, no one can be rightfully accused of misappropriating it." H.R. Rep. No. 104-788, at 7 (1996). On the other hand, taking precautionary measures to protect secrets imposes both direct and indirect costs on the owner of the secret, and thus "perfect security is not optimum security." *Rockwell Graphic Sys.*, 925 F.2d at 180 (noting that "[i]f trade secrets are protected only if their owners take extravagant, productivity-impairing measures to maintain their secrecy, the incentive to invest resources in discovering more efficient methods of production will be reduced, and with it the amount of invention"); *Lange*, 312 F.3d at 266 (noting this concern when interpreting the EEA's definition of a trade secret). Thus, while a trade secret owner need not take "every conceivable step to protect the property from misappropriation," H.R. Rep. No. 104-788, at 7, the owner must employ precautionary measures that are reasonable under the circumstances.

10. The government proved beyond a reasonable doubt that Motorola took reasonable measures to protect the secrecy of the purported trade secrets. As outlined above, the Court was presented with extensive evidence regarding Motorola's physical security. The evidence showed that Motorola carefully controlled access to the Motorola campus as well as each building on the

campus. Security cameras and alarms abounded on the campus, and there was a small force of 40 security employees to monitor the cameras and patrol the campus.

11. The Court was also presented with detailed evidence regarding Motorola's network and computer security. Motorola employed typical measures such as passwords and firewalls to prevent hackers and other outside threats from infiltrating the Motorola network. Motorola also had measures in place to protect confidential and proprietary information internally, including restricting access within the Motorola network depending on the user's authorization and the classification status of a document or file. Users of the Motorola network were reminded every time they logged onto the Motorola network that their use of the network was subject to monitoring, and that it could only be used for authorized purposes.

12. Motorola also employed a specific program, POPI, to protect its proprietary information. This program entailed detailed policies regarding the classification of proprietary documents, access to the documents, and the physical handling of the documents. Under these policies, documents containing confidential and proprietary information were marked as such, including the documents at issue here. The POPI program also provided for the training of new hires and current employees, as well as audits to promote compliance with the program's policies.

13. Motorola's final level of security consisted of agreements with Motorola employees. Motorola employees signed an employment agreement, a code of conduct understanding that contained a confidentiality provision, and a policy on the appropriate use of computer resources. Upon hiring, employees were also informed of the Motorola policy regarding the protection of proprietary information, including classification levels and their

concomitant handling requirements. Employees were reminded of their obligation to maintain the secrecy of Motorola's proprietary information through regular trainings and POPI audits.

14. The Court concludes that this multi-pronged approach to security—controlled and monitored physical access to Motorola facilities, limited access to the Motorola computer network and Motorola network equipment, a specific policy for the protection of proprietary information, and confidentiality agreements and trainings for Motorola employees—was a reasonable way to maintain the secrecy of the information in Moto 1, Moto 2, and Moto 3. *See Chung*, 659 F.3d at 825 (noting that "reasonable measures for maintaining secrecy 'have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on [a] 'need to know basis,' and controlling plant access'") (quoting Unif. Trade Secrets Act § 1 cmt., 14 U.L.A. 438, 439 (1990)). In reaching this conclusion, the Court notes that this case highlighted some gaps in Motorola's security program, as well as the ineffectiveness of some of the measures it did employ. The evidence also indicated that there were measures Motorola could have utilized to improve its security, including the monitoring of Compass and MVP for abnormal use, the regular review of employees' access authorizations, the disabling of USB ports, and the search of all bags leaving Motorola's facilities. These additional protections, however, would have come at an additional cost, and that there were other precautions Motorola could have taken does not mean that the measures it did take were not reasonable. *See Rockwell Graphic Sys.*, 925 F.2d at 180. The Court accordingly concludes that the Government proved beyond a reasonable doubt that the charged documents satisfy the second element of a trade secret.

Independent economic value

15. When evaluating the last required element of a trade secret under the EEA, courts have considered many factors in determining whether the information at issue derives independent economic value from its secrecy. Courts often consider "the degree to which the secret information confers a competitive advantage on its owner." *See, e.g., Chung*, 659 F.3d at 826-27 (holding that the information at issue derived economic value from being kept a secret because "the information could assist a competitor in understanding how [the trade secret owner] approaches problem-solving and in figuring out how to best bid on a similar project in the future"). Other courts have considered the cost and effort necessary to develop the secret information. *See, e.g., Lange*, 312 F.3d at 270 (finding that completed specifications and engineering diagrams had "considerable 'independent economic value . . . from not being generally known'" because "[e]very firm other than the original equipment manager and the [trade secret owner] had to pay dearly to devise, test, and win approval of similar parts"—a process that the specifications and diagrams would make unnecessary). In some cases, the value of the trade secret is evident in the circumstances of the offense, such as a defendant's acknowledgment that the secret is valuable or the asking price set by a defendant for the trade secret. *See id.* at 269 (noting that the defendant told his customers that "the data on offer were worth more than the asking price"); *United States v. Genovese*, 409 F. Supp. 2d 253, 257 (S.D.N.Y. 2005) (finding that because the defendant "offered the code for sale and successfully sold it, he was on notice that it derived value from its relative obscurity"). As with the other elements of a trade secret under the EEA, this is a fact-intensive analysis for which there are no bright-line rules.

16. The Court concludes that the information in the charged documents derived

economic value from its secrecy. Although the evidence before the Court indicates that the use of iDEN technology is overall on the decline, its customer base and coverage areas are still growing in certain regions of the world. When a new customer is added on the iDEN network, that customer must purchase iDEN-specific hardware from Motorola, including base stations and switching equipment. When an existing iDEN customer expands its coverage area, it must, at a minimum, purchase more base stations. This is relevant here because the information in Moto 1, Moto 2, and Moto 3 that the Court identified as secret above would be necessary for a competitor to build competing versions of these iDEN products that are sold globally. Additionally, the secret information identified above could be used to intercept messages or audio over the iDEN network. Thus, it is clear to the Court that this information derived value from its secrecy.

17. The Court has carefully evaluated each document separately and independently and certainly acknowledges that the overall economic value of each document is markedly different in the world marketplace. In particular, the overall market value of Moto 2 is rather weak because it largely details a failed project. Yet even Moto 2 describes enough useful information to have some independent economic value.

18. Jin argues that the Government also needed to prove that the information in the charged documents was not within her own personal knowledge, skill, or ability because the EEA does not apply "to individuals who seek to capitalize on the personal knowledge, skill, or abilities they may have developed" in moving from one job to another. H.R. Rep. No. 104-788, at 7. The Court agrees that the EEA allows employees to economically benefit from the general skills and knowledge that they acquired while working for a former employer. What is not permitted, however, is for employees to take confidential information about "products or

processes" from their former employers to use for their own, or a third party's, economic benefit. *See id.*; *United States v. Martin*, 228 F.3d 1, 11 (1st Cir. 2000) ("§ 1832(a) was not designed to punish competition, even when such competition relies on the know-how of former employees of a direct competitor. It *was*, however, designed to prevent those employees (and their future employers) from taking advantage of confidential information gained, discovered, copied, or taken while employed elsewhere.") Jin was accused of taking very specific technical data unique to iDEN, not broad information about telecommunications generally or skills she acquired while at Motorola. The technical data in the charged documents cannot be classified as personal or generic knowledge; it is clearly the type of "confidential information" the EEA prohibits employees from taking from their former employers.

19. Jin lastly argues that the charged trade secret documents do not qualify as trade secrets because they are labeled as "Motorola Confidential and Proprietary" instead of "Motorola Registered Secret Proprietary," and under Motorola's proprietary information classification system, a trade secret falls in the latter category. This argument fails because the statutory definition of a trade secret in the EEA—not Motorola's classification of the documents—governs the determination of whether the documents qualify as trade secrets. Of course, the definitions of the classification categories and the label ultimately given a document are evidence that is relevant to the elements of a trade secret. Motorola, however, defined "Motorola Confidential and Proprietary" information as that which an unauthorized disclosure of would cause "substantial detrimental effect" to Motorola. And, as discussed above, Motorola took many steps to protect "Motorola Confidential and Proprietary" information. That the documents at issue here are labeled as "Motorola Confidential and Proprietary" is thus not

inconsistent with them being trade secrets under the statutory definition. Accordingly, because Moto 1, Moto 2, and Moto 3 each contain some information that was not known to the public and derived value from its secrecy, and Motorola took reasonable precautions to maintain the secrecy of the information, the Court concludes that the charged documents are in fact trade secrets under the EEA.

Knowledge of the trade secrets

20. In addition to proving that the charged information qualifies as a trade secret, the Government must have proven that Jin had the requisite *mens rea* in order to establish a violation of Sections 1831(a)(3) and 1832(a)(3). Although the sections vary slightly in their *mens rea* requirements, one element the parties agree is required under both sections is that Jin had knowledge of what she possessed. What specifically Jin needs to have known about the information in her possession, however, is disputed. Jin argues that both sections require the Government to prove that she knew that the documents in her possession contained trade secrets. (R. 196, Def.'s Mem. at 4.) She does not argue that the Government needed to prove that she knew her actions were illegal under the EEA, but rather that she knew "that what she took was in fact a trade secret, as a factual matter." (*Id.* at 7.) The Government, on the other hand, contends that it only needed to prove that Jin knew the information was proprietary in order to satisfy this knowledge requirement. (R. 203, Govt. Resp. at 4.)

As an initial matter, the Court notes that this dispute arises from the lack of clarity in the case law interpreting the EEA's *mens rea* requirements. Many courts, as well as the parties here, treat the knowledge requirements in Sections 1831(a)(3) and 1832(a)(3) as one and the same

despite differences in the statutory text. The Court will accordingly analyze the sections separately.

21. Statutory interpretation begins with the plain language of the statute. *United States v. LaFaive*, 618 F.3d 613, 616 (7th Cir. 2010) (citation omitted). The Court may refer to "'the language itself, the specific context in which that language is used, and the broader context of the statute as a whole.'" *Id.* (quoting *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997)). The Court will consider the legislative history of a statute only "when necessary to decode an ambiguous enactment; it is not a *sine qua non* for enforcing a straightforward text." *DirecTV, Inc. v. Barczewski*, 604 F.3d 1004, 1008 (7th Cir. 2010). If the statute remains ambiguous after this analysis, the rule of lenity requires the statute to be interpreted in favor of the defendant. *LaFaive*, 618 F.3d at 616 (citation omitted).

22. The element of Section 1831(a)(3) at issue here requires that the defendant "knowingly . . . receives, buys, or possesses a trade secret, knowing the same to have been stolen, appropriated, obtained or converted without authorization." 18 U.S.C. § 1831(a)(3). The question here is whether "knowingly" modifies "trade secret," or only "receives, buys, or possesses." The Supreme Court was faced with an analogous question regarding a similarly structured statute in *Flores-Figueroa v. United States*, 556 U.S. 646, 129 S.Ct. 1886 (2009). In *Flores-Figueroa*, the Supreme Court interpreted a federal criminal statute forbidding "[a]ggravated identity theft" that imposes a mandatory consecutive two-year prison term upon individuals convicted of certain crimes "*if*, during (or in relation to) the commission of those other crimes, the offender '*knowingly* transfers, possesses, or uses, without lawful authority, *a means of identification of another person*.'" *Id.* at 1888 (quoting 18 U.S.C. § 1028A(a)(1)). The

Supreme Court concluded that under a plain reading of the statute, "knowingly" modifies not only the transitive verbs of "transfers, possesses, or uses," but also the object of those verbs—"a means of identification of another person." *Id.* at 1890. Because courts ordinarily interpret criminal statutes in a manner that is "fully consistent with this ordinary English usage," a phrase that introduces the elements of a crime with the word "knowingly" applies that word to each element in most criminal statutes. *Id.* at 1891; *but see United States v. Cox*, 577 F.3d 833, 837 (7th Cir. 2009) (rejecting argument that "knowingly" applies to the object of a transitive verb in 18 U.S.C. § 2423(a) given Congressional intent and that the illicit conduct in the statute was already unlawful under a related section of the statute). Accordingly, the Supreme Court held that the statute required the Government to show that the defendant knew that the means of identification at issue belonged to another person. *Flores-Figueroa*, 129 S.Ct. at 1894.

23. The Court concludes that "knowingly" in Section 1831(a)(3) modifies "trade secret," and that Section 1831(a)(3) therefore requires the Government to prove that a defendant knew, as a factual matter, that the information she possessed had the general attributes of a trade secret. The district court in the Central District of California reached the same conclusion in *United States v. Chung*, 633 F. Supp. 2d 1134 (C.D. Cal. 2009). Noting that the Supreme Court "has long recognized a presumption in favor of an intent requirement for 'the crucial element' that separates lawful from unlawful conduct," the district court concluded that it "would be unjust and inconsistent with the purpose of the criminal law to hold [the defendant] accountable for possession of what he honestly believed was publicly available information." *Id.* at 1144-45. The district court thus held that under Section 1831(a)(3), "the Government must prove that [the defendant] knew that the information he possessed was trade secret information." *Id.* at 1145.

24. The Court is not convinced, as the Government argues, that *Chung* is "an outlier" and that other cases on this issue contradict its holding that knowledge of the trade secret is a required element under Section 1831(a)(3). (R. 203, Govt Resp. at 6.) The Government is correct in noting that many courts discussing the knowledge requirement under the EEA state that the defendant must have knowledge of the proprietary nature of the information. *See, e.g., United States v. Krumrei*, 258 F.3d 535, 539 (6th Cir. 2001) (The "defendant need not have been aware of the particular security measures taken by [the trade secret owner]. Regardless of his knowledge of those specific measures, defendant knew that the information was proprietary."); *United States v. Roberts*, No:08-CR-175, 2009 WL 5449224, at *5 (E.D. Tenn. Nov. 17, 2009) (concluding that a defendant must know that the information she seeks to steal is proprietary, but does not have to know that it meets the statutory definition of a trade secret). The Government fails to acknowledge, however, that these cases deal with Section 1832(a)(3) and that the defendants were arguing that the Government needed to prove that the defendants had knowledge of the illegality of their conduct. *See, e.g., id.* Here, Jin does not argue and the Court does not conclude that the Government is required to prove that Jin knew that her conduct was illegal or that the information she possessed met the statutory definition of a trade secret.

25. The cases cited by the Government also fail to support the Government's argument because the terms "trade secret" and "proprietary information" are often used interchangeably. *See, e.g., United States v. Aleynikov*, 785 F. Supp. 2d 46, 56 (S.D.N.Y. 2011) ("To establish a violation of [Section 1832(a) of] the EEA, the Government was required to prove *inter alia* that [the defendant] acted with intent to convert proprietary source code to the economic benefit of himself [or a third party] and that he knew or intended that doing so would

injure Goldman Sachs."). For example, in *United States v. Nosal*, the district court rejected the defendant's argument that Section 1832(a) requires proof of the defendant's knowledge of the illegality of his actions, instead concluding that "it is the knowledge of the trade secrets, not the knowledge of illegal behavior, that the EEA requires." No. Cr. 08-00237, 2009 WL 981336, at *3 (N.D. Cal. Apr. 13, 2009), *rev'd on other grounds*, 642 F.3d 781 (9th Cir. 2011), *reh'g en banc granted*, 661 F.3d 781 (9th Cir. 2011)). The court went on to say, however, that allegations that the defendant knew the information he took was proprietary and that he knowingly stole and possessed the information sufficiently alleged a violation of Section 1832(a). *Id.* (emphasis added). The Government maintains that this supports its argument that it need only prove that a defendant knew that the information taken was proprietary, not a trade secret. A closer look at *Nosal*, however, indicates that the district court did not make this distinction; instead, it equated knowledge of the "proprietariness of the information" the defendant was selling with knowledge that it was a trade secret. *See id.* ("The Sixth Circuit was clear in holding that the statute was constitutional as applied to the defendant because he was well aware of the 'proprietariness of the information' he was selling, i.e., that it was a trade secret and he sought to sell it anyway. . . Likewise, in *Hsu*, the court found the statute not unconstitutional as applied to the defendant because the defendant was seeking to acquire that which he knew was not 'generally known to' or 'readily ascertainable through proper means by, the public.'") (citing *Krumrei*, 258 F.3d at 539; *United States v. Hsu*, 40 F. Supp. 2d 623, 631 (E.D. Pa. 1999)). Thus, given the plain language of Section 1831(a)(3) and the lack of clear support for the Government's argument to the contrary, the Court concludes that the Government needed to prove that Jin knew that the

information she possessed had the general attributes of a trade secret in order to establish a violation of the economic espionage provision of the EEA.

26. Seeking to avoid this result, the Government argues that "[r]equiring the Government to prove that a defendant knew the charged information was a trade secret . . . would undermine the purpose of the EEA, which was to create a comprehensive solution to economic espionage." (R. 203, Govt. Resp. at 5.) This argument fails to persuade the Court. Despite the Government's concerns, there is no requirement that a defendant must know each and every measure taken by the trade secret owner in order to have the requisite knowledge of the trade secret. Instead, it is sufficient if the defendant was aware that the information had the general attributes of a trade secret—that it was valuable to its owner because it was not generally known and that the owner had taken measures to protect it.

As the district court in *Chung* noted, this requirement "does not impose an insurmountable or even difficult burden of proof." *Chung*, 633 F. Supp. 2d at 1145. The Government need only prove that the defendant "knew the information he possessed was a trade secret, but not that he knew his behavior was illegal." *Id.* (citing *Nosal*, 2009 WL 981336, at *3). The district court continued:

> A defendant charged with economic espionage will necessarily have some understanding of the measures that have been taken to protect the information he possesses. He will know whether the facility he acquired the information from was gated. He will know if the information in his possession has proprietary, trade secret, or classified markings. If he is an employee, he will know his company's policy about whether documents can be taken home. The Government need not prove that a defendant knew all of the security measures taken to protect the information. Likewise, proving that a defendant charged with economic espionage knows that the information he possesses has economic value is not exceedingly difficult. A spy does not deal in worthless or readily ascertainable information. He collects information without authorization precisely because it has independent economic value.

Id. at 1145-46. Given this minimal burden, here, as in *Flores-Figueroa*, "concerns about practical enforceability are insufficient to outweigh the clarity of the text." 129 S.Ct. at 1893.[4]

27. Although the Court agrees with Jin that Section 1831(a)(3) requires the Government to prove that she knew that Moto 1, Moto 2, and Moto 3 contained trade secrets, this heightened knowledge requirement is easily met in this case. Jin knew that this information was not readily accessible; had she thought otherwise she would not have gone to the effort of returning to work for the few days it took her to download the documents. Jin was also aware, starting with her first day of employment with Motorola, of the many measures employed by Motorola to protect its proprietary information, and she knew that the relevant documents were marked "Confidential and Proprietary." Finally, that Jin knew this information derived economic value from its secrecy can easily be inferred from other facts. First, she had worked on iDEN and was aware of the years of research and development that went into iDEN technology. Second, Jin went through the ruse of returning to work in order to obtain the information, something she

[4] The Government's concerns about the "virtual impossib[ility]" of proving an EEA violation where the defendant did not "have an inside look at the trade secret owner's security measures" and did not "work closely with the owner to witness the restrictions on and value of the trade secret," (R. 203, Govt Resp. at 5), are also unfounded. In *United States v. Genovese*, the defendant was charged under Section 1832(a)(2) for allegedly selling source code belonging to Microsoft that briefly appeared on the internet. 409 F. Supp. 2d at 254-55. The defendant, on a motion to dismiss the indictment, argued that the definition of "trade secret" in Section 1839(3) was unconstitutionally vague as applied to his case because he found the source code at issue in the case after it had been released to the general public by a third-party. *Id.* He contended that "he could not have known that it was 'not . . . generally known to . . . the public' and that Microsoft had taken 'reasonable measures' to safeguard it." *Id.* The district court rejected this argument, finding that "a reasonable inference" from the defendant's website posting selling the source code was that "he knew the source code derived independent value because it was not 'generally known,'" and that "he knew that a third-party had 'jacked' the source code from Microsoft." *Id.* at 257-58.

would not have done had she thought the documents were worthless. These facts make it clear that Jin was aware that the charged documents had the attributes of a trade secret.

28. Turning now to the theft of trade secrets provision of the EEA, the statutory language employed in Section 1832(a)(3) is less clear in requiring that the defendant have knowledge that the information she possesses is a trade secret. Under Section 1832(a)(3), a defendant must "inten[d] to convert the trade secret," and "knowingly . . . receive[], buy[], or possess[] such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization[.]" 18 U.S.C. § 1832(a)(3). That Section 1832(a)(3) requires knowledge of "such information" instead of "a trade secret" may be a distinction without a difference, but this is an issue the Court need not decide because the Court has already concluded that the Government proved beyond a reasonable doubt that Jin knew that the charged documents were trade secrets as a factual matter.

Misappropriation of the trade secrets

29. For both theft of trade secrets and economic espionage, the Government must prove that the defendant misappropriated the trade secrets through one of the prohibited acts in Sections 1831 and 1832. Here, Jin was charged with possessing Moto 1, Moto 2, and Moto 3, knowing that they were "stolen or appropriated, obtained, or converted without authorization." 18 U.S.C. §§ 1831(a)(3), 1832(a)(3). Thus, under this element, the Government must first prove that the trade secrets at issue were actually "stolen, appropriated, or converted without authorization," and next, that Jin knew the trade secrets were "stolen, appropriated, or converted without authorization."

30. This element was met in this case. Jin downloaded and copied thousands of

documents when they were clearly outside the scope of her limited duties upon her return from sick leave. She continued to download documents even after sending her email resignation to Bach. This was in clear contravention of the Motorola policies that Jin had agreed to follow. Given the training she received as an employee of Motorola regarding the care of confidential and proprietary information, her excellent employment record and educational training, the manner in which she obtained the documents, and the lies she told the CBP and FBI agents about the documents when she was caught with them at O'Hare, the Court easily concludes that this was not an innocent mistake. The Court finds beyond a reasonable doubt that Jin knew that she had taken the documents without authorization.

The Court now turns to the unique elements of Sections 1832(a)(3) and 1831(a)(3).

Remaining theft of trade secret elements

31. As detailed herein, the Government met its burden with regards to the first three elements of Section 1832(a)(3) for Moto 1, Moto 2, and Moto 3, specifically that: the charged documents contained trade secrets; Jin knowingly possessed the charged documents, knowing they were trade secrets; and Jin knew the trade secrets were obtained without authorization. It was also undisputed at trial that the trade secrets related to a product placed in interstate commerce. The Court now turns to the two remaining elements under Section 1832(a)(3).

Intent to provide an economic benefit to the defendant or a third party

32. The fourth element under Section 1832(a)(3)—that the defendant intended for the offense to economically benefit anyone other than the owner—ensures that mere possession of trade secrets is not unlawful. Instead, the Government must have proven that Jin possessed the trade secrets with the intent to convert the trade secrets to the economic benefit of herself or

someone else who is not the trade secret's owner. *See Hsu*, 155 F.3d at 195; H.R. Rep. 104-788, at 11; S. Rep. 104-359, at 13 (1996).

Jin contends that this element requires the Government to "prove an economic benefit to the end user—whether the end user is the defendant herself or a third party to whom the Government has proven the defendant intended to provide the materials." (R. 196, Def.'s Mem. at 3.) Based on this premise, Jin maintains that if the Government's theory of the case was that Jin took the documents for her own benefit, then the Government needed to prove that the trade secrets provided Jin with information she did not already possess. (*Id.* at 3.) If the Government's theory was that Jin intended to benefit a third party by taking the charged documents, Jin argues that the Government "needed to prove that the third party stood to profit in some manner from the three charged documents." (*Id.* at 4.)

33. The Court concludes that this argument overstates the Government's burden under Section 1832(a)(3). The statutory language and the case law interpreting it establish that the key inquiry is the defendant's intent at the time of the offense, not whether there was an actual benefit to a party other than the owner of the trade secret. *See Hsu*, 155 F.3d at 196 ("[P]rosecutions under § 1832 uniquely require that the defendant intend to confer an economic benefit on the defendant or another person or entity."). Additionally, while the Court agrees that the EEA permits an employee to use the general skills and knowledge she acquired working for a previous employer to her economic benefit, as previously discussed, what is at issue here is not general information or knowledge that Jin possessed but rather specific technical information unique to iDEN.

34. In this case, the Court concludes that this element was proven beyond a reasonable

doubt because Jin took the trade secrets to help her prepare for her future employment. It is clear that when Jin was stopped with the documents on February 28, 2007, she had planned to move to China for an indefinite duration and work for Sun Kaisens. Although Jin had been an excellent employee at Motorola throughout most of her time there, after her prolonged and serious illness, Jin had decided to return to China to be closer to her husband and her ailing mother. The evidence clearly showed that employment at Sun Kaisens was key to this plan. There is no doubt that Jin had done work for Sun Kaisens in the past, and her emails with Sun Kaisens management and her former supervisor at Lemko establish that she planned to work for Sun Kaisens upon her return to China.

35. Jin also clearly believed that the documents she took from Motorola—including the trade secrets—would help her prepare for her future employment at Sun Kaisens. While the evidence did not establish that someone at Sun Kaisens had requested the documents or that Jin planned to give the documents to Sun Kaisens, the evidence demonstrated beyond a reasonable doubt that, at a minimum, Jin planned to use the documents to prepare herself for her position at Sun Kaisens. She admitted numerous times, including in her written statement, that she sought to refresh her memory with the documents and to use them to help her get her next job. After being on medical leave from Motorola for 15 of the preceding 21 months, Jin could not arrive at Sun Kaisens unfamiliar with the very areas of technology that she had told Gengshan Liu she had worked on at Motorola. Thus, while there was no evidence regarding what the actual economic benefit to Jin would be in terms of a dollar amount, it is clear that she planned to use the documents to her economic benefit by using them to prepare for her next job at Sun Kaisens. Jin's planned use of these documents would also indirectly benefit Sun Kaisens.

36. In reaching this conclusion, the Court notes that there was no evidence that Sun Kaisens sought this information, and in fact, the evidence indicated that Sun Kaisens would likely not be directly interested in iDEN technology because it was focused on more advanced CDMA technology. The focus here, however, is on Jin's intent, and the evidence showed that Jin had made representations about her work at Motorola to Gengshan Liu, and that she sought to be a productive, helpful member of his team. Thus, even though in the end Jin's knowledge of iDEN technology and the stolen trade secrets may not have directly benefitted Sun Kaisens, she believed at the time she took the documents that they would, at a minimum, help prepare her for her new job with Sun Kaisens and meet the expectations of her new employer.

37. The conclusion that Jin planned to use the documents for this improper purpose is also supported by the many misrepresentations she made leading up to and following her arrest, the sheer quantity of documents she took, and the manner in which she took them. First, Jin lied to Motorola employees in the course of her phony return to work. The evidence showed that Jin never intended to return to work for Motorola and instead returned from medical leave solely to obtain the documents that were found in her possession on February 28, 2007. Jin also lied repeatedly to CBP and FBI officials about her employment with Motorola, the source of the documents, and her contacts in China.

38. Jin's vast downloading of thousands of documents over the course of a few days also indicates that she did not merely clean out her desk in a haphazard manner. She had multiple copies of Moto 1, Moto 2, and Moto 3 in her possession when she was stopped at O'Hare. She used multiple storage devices to store the documents, and possessed many of the documents in paper form. These facts indicate a concerted effort on the part of Jin to obtain

information she believed would help her in her future job.

39. The elaborate steps taken by Jin to obtain the documents also show that she was acting with the improper purpose of obtaining an economic benefit for herself. Her prior purchase of a one-way ticket to China indicates that she had no intention of staying when she returned to Motorola. As soon as she knew she had access to the Motorola buildings and the Motorola network, she began accessing and saving thousands of documents, and did so late into the night and after she sent her email resignation. There simply was no legitimate reason for these multiple deceptive acts, which firmly establish Jin's criminal intent. The Court concludes that the Government proved beyond a reasonable doubt that Jin took the trade secrets with the purpose of economically benefitting herself and indirectly benefitting Sun Kaisens.

Intent to injure the owner of the trade secret

40. A defendant guilty of theft of trade secrets must have intended or known that her conduct would harm the owner of the trade secret. The legislative history of the EEA suggests that this requires that the defendant "knew or was aware to a practical certainty" that her conduct would cause injury to the trade secret's owner. *Hsu*, 155 F.3d at 196 (quoting S. Rep. No. 104-359, at 15). This does not mean that the Government must "prove malice or evil intent, but merely that the actor knew or was aware to a practical certainty that his conduct would cause some disadvantage to the rightful owner." H.R. Rep. No. 104-788, at 11; *see also Aleynikov*, 785 F. Supp. 2d at 59 (intent to harm trade secret owner established by evidence that the stolen trade secrets could be used to directly compete with the trade secret owner, the defendant knew of the highly secretive nature of the business area and of the measures taken to protect the trade secrets, and that the defendant took steps to circumvent the security measures).

41. Here, this element is satisfied because Jin was well-informed that her conduct would harm Motorola. First, as discussed above, Jin knew the charged documents were trade secrets because she was aware that information within the documents was not available to the public, that the information derived value from its secrecy, and that Motorola took many precautions to maintain the secrecy of the information. All of the charged documents are marked as "Motorola Confidential and Proprietary," and Motorola's policy regarding the protection of proprietary information, a copy of which was in Jin's possession on February 27, 2007, states that the unauthorized disclosure of "Motorola Confidential and Proprietary" information "would cause substantial detrimental effect" to Motorola. Additionally, the following statement is found on the covers of both Moto 1 and Moto 2: "The information contained in this document is classified Company Confidential. The use and divulgence of any part of this information can seriously affect the welfare and financial security of the company."

42. Second, Jin, as a former Motorola employee, knew of the effort and resources that went into developing and protecting the technology described in the trade secrets, and she therefore knew that the use or disclosure of the information could give an unfair advantage to a Motorola competitor, thereby harming Motorola. Additionally, even if the trade secret information never reached the hands of a competitor, the possibility that it could would cause Motorola to take preventative measures to reduce the damage a potential disclosure might cause. Thus, the Court concludes that the Government proved the final element under the theft of trade secrets statute. The Court therefore finds that the Government proved beyond a reasonable doubt that Jin is guilty of Counts One, Two, and Three of the indictment.

Remaining economic espionage element

43. As discussed above, the Government proved the first three elements under Section 1831(a)(3) beyond a reasonable doubt. The remaining issue under Section 1831(a)(3) is an additional *mens rea* element necessary to establish a violation of the economic espionage provision of the EEA—that Jin knew or intended that her conduct would benefit a foreign Government or a foreign instrumentality. This element has two related parts: the intended beneficiary and the intended benefit. The Government must first prove that the intended beneficiary was a "foreign Government, instrumentality, or agent." 18 U.S.C. § 1831(a). Here, the Government alleged that Jin intended for her conduct to benefit the PRC, which is clearly a foreign Government.

44. Second, the Government must prove that Jin intended or knew that her conduct would benefit the PRC. While Section 1832 limits the type of "benefit" intended to economic benefits, "benefit in Section 1831 is intended to be interpreted broadly." H.R. Rep. No. 104-788, at 11. The defendant need not intend to confer an economic benefit; rather the Government need only prove that the defendant intended that her actions would benefit the foreign Government, instrumentality, or agent "in any way." *Id.* "Therefore, in this circumstance, benefit means not only an economic benefit but also reputational, strategic, or tactical benefit." *Id.*

45. Here, the government did not prove beyond a reasonable doubt that Jin intended or knew her conduct would benefit the PRC in any way. The Government put forth no evidence that Jin was asked or directed to take the trade secrets, and as discussed above, the evidence did not establish that Jin planned to give the trade secrets to Sun Kaisens, let alone the PRC. Instead, the Government argued that Jin knew her conduct would benefit the PRC because Sun Kaisens develops telecommunications technology for the Chinese military, Jin knew that Sun Kaisens

developed telecommunication projects for the Chinese military, and the trade secrets pertained to telecommunications technology.

46. The inferential chain from the facts to the Government's conclusion fails to establish the required proof beyond a reasonable doubt. First, the same evidence that the Government relied on to show that Jin knew that Sun Kaisens develops technology for the Chinese military also showed that the Chinese military was seeking telecommunications technology that was superior to and incompatible with iDEN. Nearly all of the documents found in Jin's possession pertain to telecommunications systems that use CDMA, soft switching technology, or have other technological requirements that could not be met using iDEN. Additionally, the evidence before the Court established that while iDEN technology was still generating revenue for Motorola in 2007, it was 2G technology that had been surpassed by other telecommunications technology and would likely be phased out of use in the not-too-distant future. Thus, this was not cutting-edge technology that would necessarily give the PRC any tactical, reputational, or other benefit.

Second, the only purported evidence of any connection or link between the Chinese military and the trade secrets in the documents does not meet the Government's burden. The Government pointed to two Chinese military documents that contain a total of three brief references to telecommunications systems using channel widths of 25 and 50 kilohertz. While iDEN technology is hypothetically compatible with those channel widths, the Government failed to show why the Chinese military would want to use iDEN when the publically available and technologically superior TETRA technology could also be used in such systems. There was also a passing mention of Israel's "Secure Cellular Phone Applications" on a slide in a Chinese

military telecommunications presentation, but the slide does not mention anything about iDEN and the same presentation discusses China's GSM and CDMA mobile communication networks. That these minor references to technology that could possibly relate to iDEN indicate a connection between the Chinese military or the PRC and iDEN is a stretch at best. Given the superiority of other available telecommunications technology to iDEN, the Chinese military documents' focus on technologies that are incompatible with iDEN, and, at best, minimal evidence of a connection between the Chinese military documents Jin had in her possession and Moto 1, Moto 2, and Moto 3, the Court concludes that the evidence failed to establish beyond a reasonable doubt that Jin intended or knew that her conduct would benefit the PRC. There is certainly plenty of speculative proof that the PRC may have benefitted from Jin's conduct, but such speculation does not equate to proof beyond a reasonable doubt. The Court therefore finds that the Government did not prove beyond a reasonable doubt that Jin is guilty of Counts Four, Five, and Six of the pending indictment.

CONCLUSION

For the foregoing reasons, the Court finds that the Government proved beyond a reasonable doubt that Jin is guilty of theft of trade secrets under Section 1832(a)(3) of the EEA. The Government's evidence failed to prove beyond a reasonable doubt that Jin is guilty of economic espionage under Section 1831(a)(3) of the EEA. The Court hereby enters a judgment of guilty against Jin on Counts One, Two, and Three, and a judgment of not guilty on Counts Four, Five, and Six of the pending indictment.

The Court will set a tentative sentencing date of April 18, 2012, at 1:00 p.m.

Entered:

Judge Ruben Castillo
United States District Court

Dated: February 8, 2012